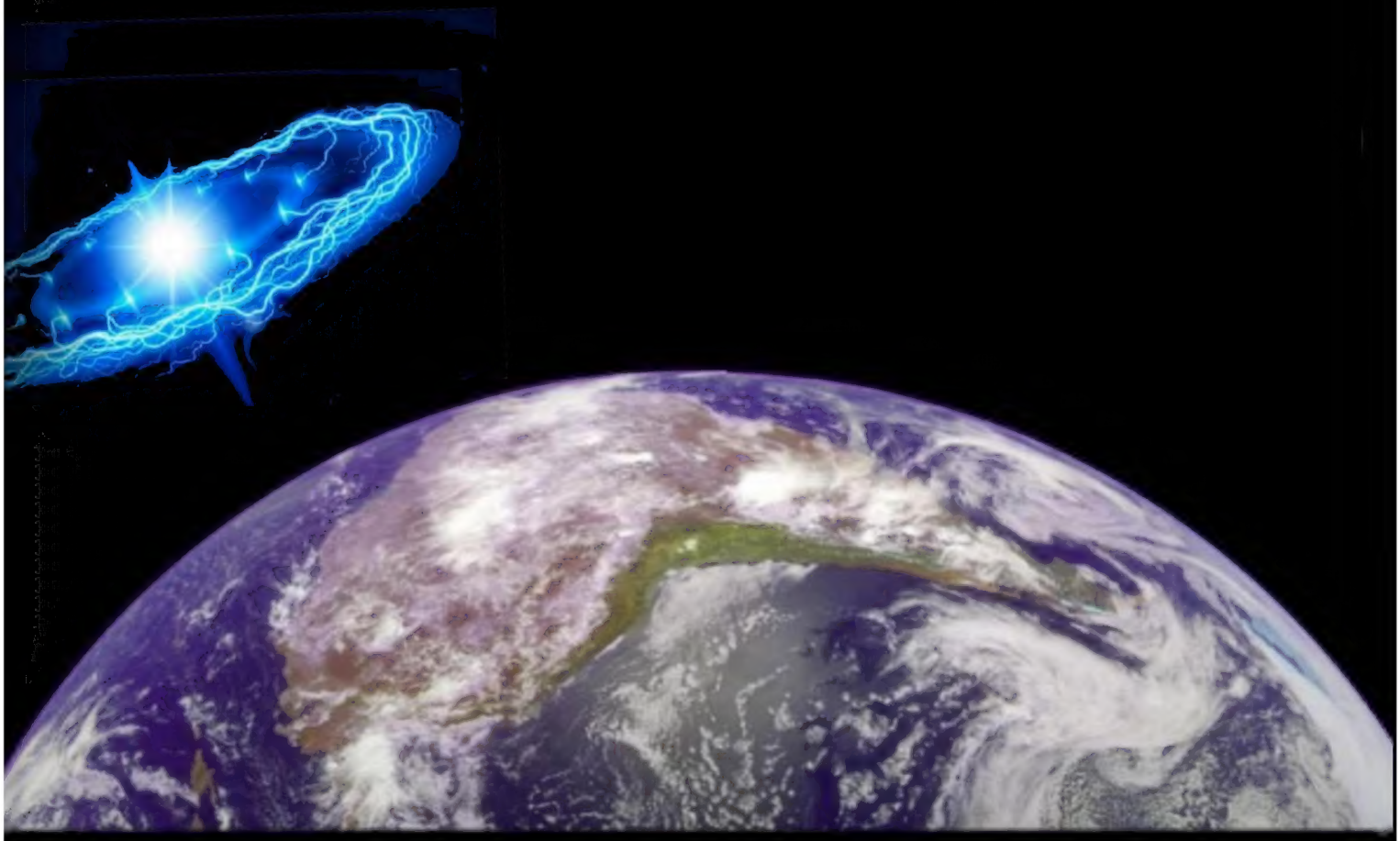


Vladimir Gurevich

Paradoxes of the problem of critical infrastructure protection against EMP: the truth is out there

Haifa

2023

V. Gurevich

Paradoxes of the problem of critical infrastructure protection against EMP: the truth is out there. – Haifa, 2023.

This small book is the continuation of previously published books by the author on the problem of nuclear EMP (HEMP).

A paradoxical situation is described, including expensive fakes, bureaucratic tricks, and simply misconceptions in the field of protecting critical infrastructure from nuclear EMP.

The book contains criticism of existing trends in the problem of protecting critical infrastructure against EMP and explains the author's opinion regarding some essential EMP issues, since it differs from the currently accepted view, and also author's general concept (strategy) of critical infrastructure protection against EMP.

The book is intended for EMP experts, for politicians, government officials, heads of enterprises and research organizations, and may also be of interest to professors and teachers of universities and students.

CONTENTS

Preface

Having worked for many years in the field of HEMP protection of critical civilian electrical equipment, I have had the opportunity to read hundreds of reports and articles on this topic, take part in conferences, and correspond with the world's leading experts in this field. As I progressed in this field, I accumulated more and more questions and doubts that I could not get answers to from leading experts.

The main question and the main paradox are that in the presence of hundreds of reports written over more than 50 years by dozens of the world's leading corporations and the availability of hundreds of types of all kinds of HEMP protection means on the free market, the critical infrastructure of all countries of the world without exception remains unprotected.

Two small substations in the United States, partially equipped with protective equipment many years ago, do not count. In addition, for some reason, these means of protection are treated there as top-secret information, not allowing anything to be photographed and recorded even by rare visitors who have special permission to visit these substations.

And when I asked a question about this strange situation to the head of one of the American consulting companies specializing in this field, I was accused of asking provocative questions specifically to discredit this company, and also demanded to apologize! Isn't that a paradox?

Gradually, I gathered a fairly large collection of all sorts of paradoxes in this area and a fairly complete picture of the current situation appeared, including expensive fakes, bureaucratic tricks and a complete lack of desire for a real solution to the problem.

It is likely that some EMP professionals, government officials, executives of energy, water and communications companies are not fully aware of the situation and do not understand the reason for this state of affairs. This is confirmed by the numerous perplexed statements of such leaders.

Especially for the above-mentioned category of managers, as well as for all those interested in this topic, I wrote this small book, in which I analyzed the current paradoxical situation and presented recommendations for correcting the situation.

Specific technical solutions to protect critical infrastructure from EMP have been described in my previously published books.

I hope that my work will not be in vain.

Questions and comments can be sent to: vladimir.gurevich@outlook.com or vladimir.gurevich@gmail.com

Chapter I

Everybody Understands Everything...

I have published many books on various technical problems, including several books describing specific practical solutions to the technical problems of protecting critical infrastructure from High Altitude Electromagnetic Pulse (HEMP), Fig. 1.1:

Fig. 1.1. Some my books describing specific practical solutions to the technical problems of protecting critical infrastructure from High Altitude Electromagnetic Pulse (HEMP).

- Protection of Substation Critical Equipment Against Intentional Electromagnetic Threats;
- Cyber and Electromagnetic Threats in Modern Relay Protection;
- הגנת ציודים של תחמ"ש מפני דופק אלקטרומגנטי
- Protecting Electrical Equipment. Good Practices for Preventing High Altitude Electromagnetic Pulse Impacts;
- Protecting Electrical Equipment. New Practices for Preventing High Altitude Electromagnetic Pulse Impacts;
- Nuclear Electromagnetic Pulse: Practical Guide for Protection of Critical Infrastructure.

The practical focus of these books differentiated it's from all other books on the same subject available on the market. Instead of discussing general HEMP threats to the national infrastructure and pen-picturing the disasters and destructions usually dominating the books on this subject, Fig. 1.2.

Fig. 1.2. Several books (out of dozens on the book market) in different languages, colorfully describing in detail the disasters, destruction, economic damage that will befall the country after the HEMP attack, as well as the bureaucratic games of civil and military officials responsible for protecting infrastructure against HEMP.

Unfortunately, the scientific reports, Fig. 1.3, of the leading research centers (such as Idaho National Laboratories, Oak Ridge National Laboratories, Lawrence Livermore National Laboratory, NERC, etc.) have not deviated very far from these books in the sense that they also do not contain real practical developments and recommendations sufficient for the practical implementation of infrastructure protection.

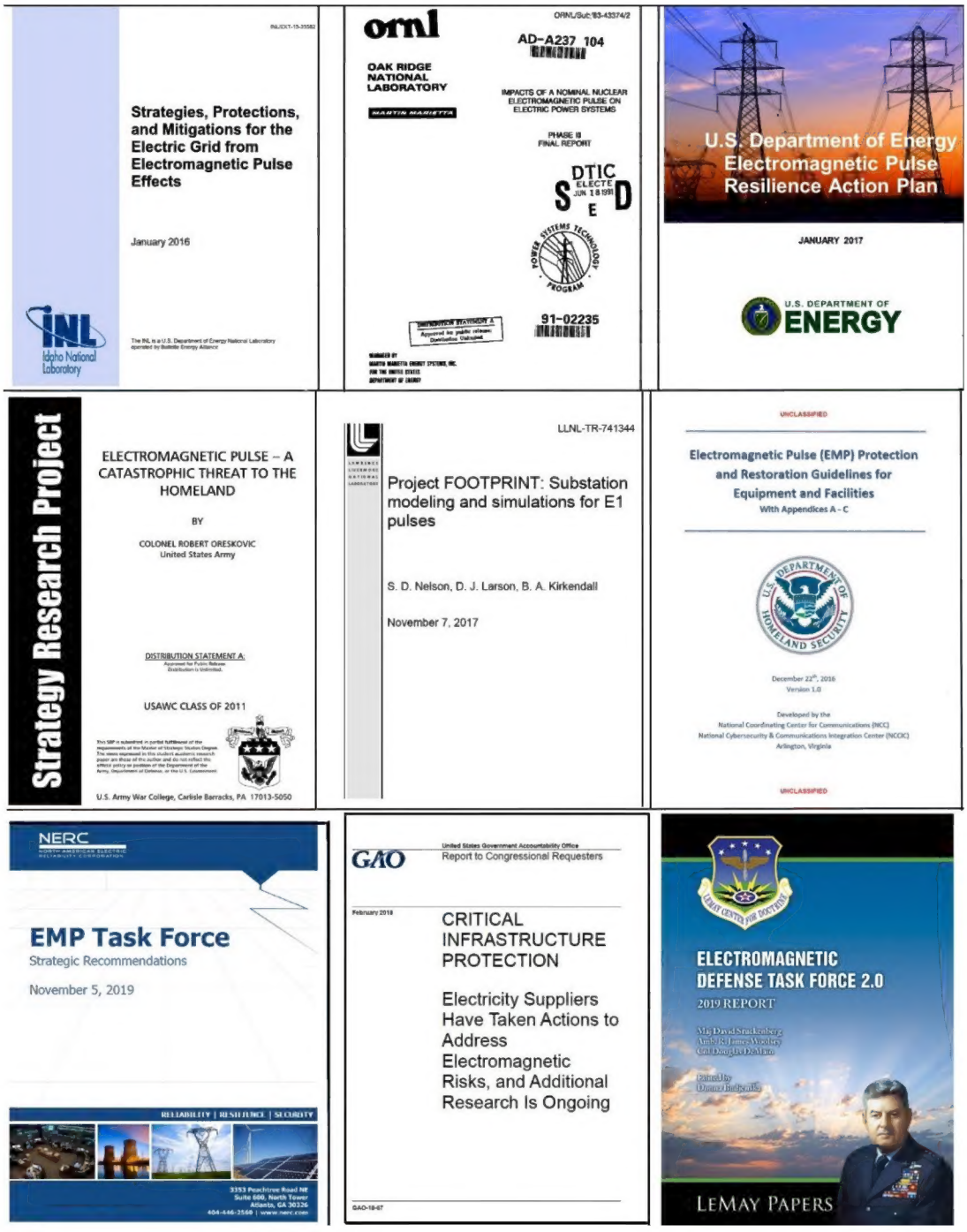


Fig. 1.3. Some scientific reports of the leading research centers on the topic of HEMP.

My books listed above represent practical recommendations on protecting certain types of electrical equipment against HEMP. So, I thought that such clear and practical recommendations unavailable before were exactly what everybody needed — both HEMP experts and power systems staff. Thus, I enthusiastically sent out the information about these books to all world-leading experts on HEMP. As a result, nearly a hundred experts have bought the book. Seemingly, I should be delighted with such popularity amongst experts and their interest in my work.

However, something prevents me from feeling delighted. To be more specific, there was an absolute indifference and lack of interest shown to the proposed practical protection means. It was strange as some of the topics covered in the book were controversial, and my conclusions and recommendations did not coincide with generally accepted views. e.g.:

- grounding does not protect electrical equipment against HEMP;
- cable shields should be grounded using the additional capacitance and inductance;
- the construction of protecting devices and elements usually selected for the protection of electronics against the E1 component of HEMP are not reasonable or correct;
- special HEMP-filters advertised as the basic means for the protection of the equipment against HEMP are not suitable;
- methods and results of digital protective relays tests published in technical literature prove the test inadequacy.

Such conclusions should have caused wariness, hard questions, disputes, disagreement, if not a total denial. I expected at least some reaction to the measures and remedies proposed, to the conclusions controversial to the existing practice ... But I did not receive any critical comment!

Not a single comment! Isn't it strange?

However, my communication with the representative of one of the American companies receiving public contracts on research in the HEMP protection field was even stranger. That representative raised the question of the great importance and relevance of the protection of power transformers of power systems from HEMP, and of the necessity of extensive and serious research and adequate funding, and he asked me to confirm that. However, as soon as I told him that I have a simple and reliable solution, the representative lost any interest in further discussion and has not even asked me what kind of solution I could propose.

Thus, the practical solution to the problem was not interesting at all. That is, on the one hand, the number of organizations dealing with this problem and receiving money from budgets increases extremely (especially in the USA), and on the other hand, no organization shows a spark of interest in practical solutions. Rather, the opposite is true: everyone wants to preserve the status quo as long as possible, that is, to have no concrete, simple, and affordable practical solutions. They have commercialized this issue and now it represents a well-functioning business. Dozens of professional consultants who frighten people with HEMP consequences appeared there during the last 10-20 years. Dozens of books, hundreds of reports have been published on this topic. Dozens of private and state-owned organizations have received orders to conduct research in this field. Below is a non-exhaustive list of them (for USA only!):

- Metatech Corp.
- Department of Homeland Security (DHS)
- EMP Commission of Congress
- North American Electric Reliability Corp. (NERC)

- Department of Energy
- Department of Defense (DoD)
- Critical Infrastructure Partnership Advisory Council (CIPAC)
- Electric Infrastructure Security Council (EICS)
- Defense Science Board (DSB)
- US Strategic Command (USSTRATCOM)
- Defense Threat Reduction Agency (DTRA)
- Defense Logistics Agency (DLA)
- Air Force Weapons Laboratory
- FBI
- Sandia National Laboratories
- Lawrence Livermore National Laboratory (LINL)
- Oak Ridge National Laboratory
- Idaho National Laboratories
- Los Alamos National Laboratories
- Martin Marietta Energy Systems, Inc.
- National Security Telecommunications Advisory Committee
- Federal Emergency Management Agency (FEMA)
- National Academy of Science
- Task Force on National and Homeland Security
- House Armed Services Committee (HASC)
- EMPrimus
- SARA Inc.
- Neighborhood of Alternative Homes (NOAH)
- EMPact America
- Federal Energy Regulatory Commission (FERC)
- Electric Power Research Institute (EPRI)
- NASA
- U.S. Northern Command (NORTHCOM)
- SHIELD Act
- EMP Grid Servicies
- EMP Technology Holding
- Field Management Services
- Strategic National Risk Assessment (SNRA)
- Walpole Fire Department
- Act for America
- DipiPlex
- CASI
- EMP Engineering
- Roxtec International
- Hardened Structures
- Small Business Innovation Research (SBIR)
- Secure the Grid Coalition
- JINSA's Gemunder Center EMP Task Force
- CENTRA Technology, Inc
- Page
- Federation of American Scientists
- Logistics Management Institute
- DVO Consulting
- MDW Associates
- The Defense Systems Information Analysis Center (DSIAC)

Moreover, that list does not include large defense corporations such as Raytheon, Lockheed, General Dynamics, Northrop, Parsons, etc., universities dealing with this topic, as well as numerous manufacturers of all kinds of protection against HEMP (filters, screens, protected rooms, bunkers, etc.) and test centers.

Some companies are seriously dealing with this problem and accomplished significant achievements in this area. Unfortunately, in most of these companies, the topic of protecting civil infrastructure is not separated from topics such as Tempest, secured communications, anti-terrorism protection, radio frequency weapons, and other secret and top-secret topics. All these topics are being developed by the same companies, in parallel by the same specialists. Therefore, the topic of protecting civil infrastructure requires same active top-secret clearance with SCI eligibility, as well as real secret topics, Fig. 1.4.


PARSONS

ELECTROMAGNETIC (EMP) PROTECTION SPECIALIST

Company Name:
Parsons

Security Clearance:
Top Secret / SCI

Location:
Fort Belvoir, Virginia

Country:
United States

Minimum Clearance Required to Start:

Top Secret SCI

Job Description:

The EMP Specialist identifies all aspects of electromagnetic (EM)-related vulnerabilities, increases the customer's awareness of potential vulnerabilities and impacts of EM on mission execution capability, and provides recommendations to mitigate or eliminate identified vulnerabilities. Additionally, the EMP Specialist performs EMP verification of onsite steel room construction IAW MIL STD 188-125-1.

any of the following EM pathways: electrical power systems, building, lighting, and equipment grounding to include tempest accreditation; adequately secured and non-secured communications

Fig. 1.4. Part of requirements and job description for EMP protection specialists in Parsons Corp.

This is a serious problem, since all non-secret developments in the field of civil infrastructure protection remain unknown to civilian specialists, in particular in the field of electric power. In this case, the reason for the lack of practical solutions for the problem among civilian specialists is different, but the result is the same.

Recently, adventurous and smart businessmen have "invented" a new term: “Cyber and Electromagnetic Activity (CEMA)” merging widely different problems of cybersecurity and protection of infrastructure against HEMP. Immediately new organizations emerged ready to "saw" the new budgets:

- National Cybersecurity and Communication Integration Center (NCCIC)
- Cybersecurity & Infrastructure Security Agency
- Critical Infrastructure and Key Resources (CIKR)
- National Coordination Center for Communications (NCC)
- AcquSight

like many and many others...

At one of the lectures for civilian and military experts, organized by the head of one of the above organizations from the United States, the speaker very colorfully described the burning-out of large transformers under the geomagnetic currents induced by solar storm and HEMP, emphasizing the enormous complexity of protection. At the end of the lecture, I requested to speak and was kindly invited to the podium. However, as soon as I pointed out that solar storms are significantly different from the HEMP and it is not that difficult to protect the power transformer against HEMP, I was interrupted and informed that the lecture was finished and asked me to come down from the podium. Then, the lecturer came to me and asked in a low voice: "Why do you argue? We just frightened them a little, it was for your benefit, too!"

Okay....So, everybody understands everything...But what do they say?

Future conflicts will be won in a new arena — that of the electromagnetic spectrum and cyberspace. We must merge, then master those realms.

Admiral Jonathan W. Greenert,
U.S. Navy

Our power grid is very vulnerable. It's very much on edge. Our military knows that.

Roscoe Bartlett,
Ex-Congressmen

Our vulnerability is increasing daily as our use of and dependence on electronics continues to grow in both our civil and military sectors

...under the Obama Administration the Department of Energy has been part of the problem, not part of the solution to protecting the nation's electric grid from the existential threat that is EMP

Dr. William R. Graham,
Chairman of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP)

The problem is not the technology. We know how to protect against it. It's not the money, it doesn't cost that much. The problem is the politics. It always seems to be the politics that gets in the way.

We have been trying to get Congress for years to harden the electric grid because there is no excuse for being vulnerable to these threats. The Department of Defense has known for 50 years for how to protect its systems but we never did that for the civilian power grid.

...its potentially paralyzing effects on military forces and civilian critical infrastructures were deeply understood only by a small number of nuclear strategists and specialists.

Dr. Peter Vincent Pry,
Executive Director of the Task Force on National and Homeland Security

It would be "suicidally optimistic" to assume that an EMP attack that inflicted a state-wide blackout would not also cause cascading grid and infrastructure failures at least regionally.

Dr. William Radasky,
Founder and President of the Metatech Corporation

The current state of EMP protection is random, disoriented and uncoordinated.

Dr. George H. Baker,
Prof. Emeritus James Madison University

American society has grown so dependent on computer and other electrical systems that we have created our own Achilles' heel of vulnerability, ironically much greater than those of other, less developed nations. When deprived of power, we are in many ways helpless, as the New York City blackout made clear. In that case, power was restored quickly because adjacent areas could provide help. But a large-scale burnout caused by a broad EMP attack would create a much more difficult situation. Not only would there be nobody nearby to help, it could take years to replace destroyed equipment.

Jon Llewellyn Kyl
Senator from Arizona

Army, NAVY and Strategic command continue to think that they need to think about the problem

Dr. Ashton B. Carter,
Former Secretary of Defense

I don't mean to be so flippant, but there really aren't any solutions to THIS, so I would just leave it at that

General M. V. Hayden
Ex-Director of the National Security Agency (NSA);
Ex-Director of the Central Intelligence Agency (CIA)

"I don't think we have an illusion we will prevent it. That's really the government's job"

Mike Bryson,
Vice president of operations for the Valley Forge, Pennsylvania-based operator

---

"Managing that kind of threat right now — no one really has the resources to do that"

Richard Mroz,
President of the New Jersey Board of Public Utilities

"Much of the available information is not specifically applied to electric utilities, making it very difficult for utilities and regulators to understand effective options for protecting energy infrastructure".

Robin Manning,
Vice president for transmission and distribution for the Electric Power Research Institute (EPRI)

"The potential impacts of GMD and HEMP are real; however, evaluating the effects of such events on existing and future power grid infrastructure is complicated and requires concrete, scientifically-based analysis. Once the true impacts are known, including the potential unintended consequences of some mitigation options, cost effective mitigation and/or recovery options can be developed and employed".

Dr. Randy Horton,
Senior Program Manager, Electric Power Research Institute (EPRI)

The time for research is running out; we have the data we need. It's time for bold actions

R. James Woolsey,
former Director Central Intelligence Agency (CIA)

On the one hand, while HEMP experts understand everything, they want to delay solving particular technical problems as long as possible. On the other hand, power system experts want those technical problems to be solved by somebody else, e.g. by the military. Indeed, why do they have to deal with additional obscure problems while they have their own immediate challenges? So, let us leave the problems at that. The library department of the energy company I work for bought two copies of the mentioned monograph (Part 1) and informed all department's heads and colleagues about that. But none out of the several thousand employees of the company took an interest in the book, apart from reading it. While rhetorically everyone is very interested in solving this problem and they spend a lot of money for world-leading lecturers to explain very general things, the reality is different...It is paradoxical...

However, in 2019 following the decades of lukewarm processes, usual bureaucratic back-door games at all levels, and quiet businesses of hundreds of people were enjoying the profits which ended suddenly. Change occurred by the long-awaited document signed by USA President Donald Trump: "Executive Order on Coordination National Resilience to Electromagnetic Pulses", see Fig. 1.4. Fortunately, the Golden Era had begun and all those bureaucrats who used to shuffle this important issue under the rug finally took the matter seriously and focused on it! Isn't that a fact? No, since that document was prepared by the same bureaucrats and aimed to further amplification of the mentioned "educational" and "explorative" activities oriented to public finance grantsmanship, instead of dealing with the particular problems. Just read the quotes below to understand the focus of that publication:

FROM WHITEHOUSE.GOV

Executive Order on Coordinating National Resilience to Electromagnetic Pulses

INFRASTRUCTURE & TECHNOLOGY

Issued on: March 26, 2019

Fig. 1.5. Executive Order signed by President D. Trump

…***conduct R&D and testing to understand the effects of EMPs*** on Department of Defense systems and infrastructure, improve capabilities to model and simulate the environments and effects of EMPs, and ***develop technologies to protect Department of Defense systems and infrastructure from the effects of EMPs*** to ensure the successful execution of Department of Defense missions;

…***share technical expertise and data regarding EMPs*** and their potential effects with other agencies and with the private sector, as appropriate;

The Secretary of Energy shall conduct ***early-stage R&D, develop pilot programs***, and partner with other agencies and the private sector, as appropriate, ***to characterize sources of EMPs and their couplings to the electric power grid*** and its subcomponents, understand associated potential failure modes for the energy sector, and coordinate preparedness and mitigation measures with energy sector partners.

…in coordination with the heads of relevant SSAs, ***conduct R&D to better understand and more effectively model the effects of EMPs*** on national critical functions and associated critical infrastructure…

Within 1 year of the date of this order, and as appropriate thereafter, the Secretary of Energy, in consultation with the heads of other agencies and the private sector, as appropriate, ***shall review existing standards for EMPs*** and develop or update, as necessary, quantitative benchmarks that sufficiently describe the physical characteristics of EMPs, including waveform and intensity, in a form that is useful to and can be shared with owners and operators of critical infrastructure.

Within 1 year of the date of this order, and every 2 years thereafter, the Secretary of Homeland Security, in coordination with the Secretaries of Defense and Energy … ***shall submit to the President, through the APNSA, a report that analyzes the technology options available to improve the resilience of critical infrastructure to the effects of EMPs.***

Within 180 days of the completion of the activities directed by…, the Secretary of Homeland Security … ***shall develop and implement a pilot test to evaluate available***

engineering approaches for mitigating the effects of EMPs on the most vulnerable critical infrastructure systems, networks.

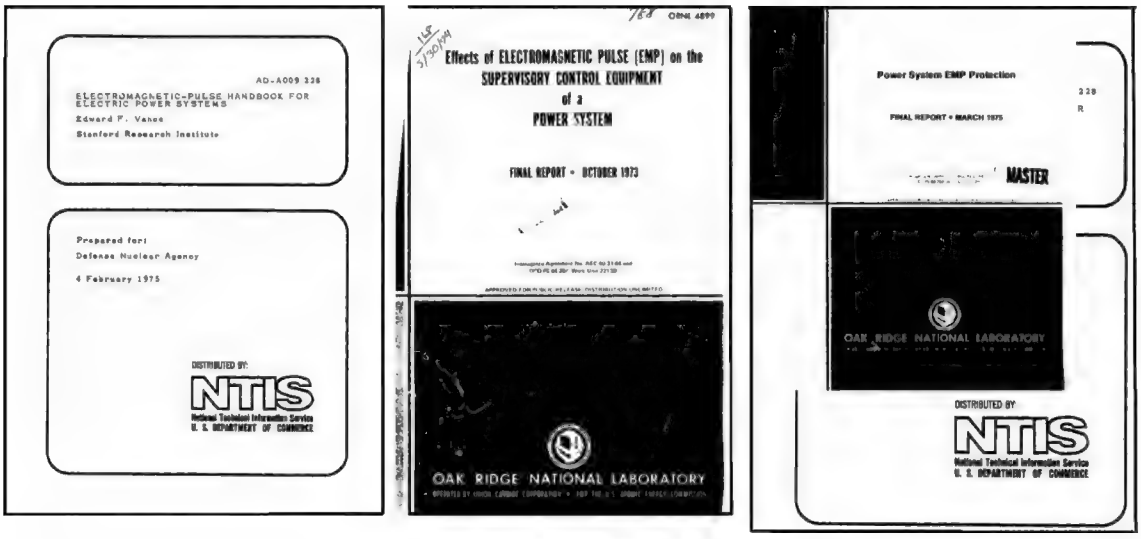


Fig. 1.6. Forty-five-year-old EMP reports: “Electromagnetic Pulse Handbook for Electric Power Systems”, 1975 (Stanford Research Institute); “Effect of Electromagnetic Pulse (EMP) on the Supervisory Control Equipment of a Power System”, 1973 (Oak Ridge National Laboratory); “Power System EMP Protection”, 1975 (Oak Ridge National Laboratory).

«***R & D to better understand***»?! And this after 45 years of research on HEMP, reflected in hundreds of publicly available scientific reports, a partial list of which on 6 pages was given in Appendices "B" and "C" of the first part of mentioned monograph?! With the money from the state budget, officials decided to start reading yellowed from time reports (Fig. 1.6)?

Is there a problem with standards? Appendix "A" of the mentioned first part of the monograph contains a long list of civil and military standards in the field of HEMP. Editing and updating of these standards is carried out as necessary by the relevant international working groups without any connection with the “Executive Order”!

Fig. 1.7. Report of U.S. Department of Homeland Security (DHS) on the Executive Order realization.

What is the document itself, such is the report on its implementation (Fig. 1.7):

"The Department Homeland Security (DHS) is actively updating the EMP guidelines and anticipates reissuing in fiscal year 2020.

The DHS Science and Technology Directorate (S&T) developed a technology scouting report, ***cataloguing a number of available EMP protection equipment and testing organizations***. This report highlights the variety of commercial equipment available to protect against an EMP. The initial version of this report was completed in June 2020 and will be available to federal agencies and private sector partners through the Homeland Security Information Network (HSIN).

As funding becomes available, S&T, in coordination with CISA, will conduct ***vulnerability testing of prioritized critical infrastructure components***, as well as validation testing of potentially applicable mitigation options for those components in order to better inform critical infrastructure owners and operators on what actions they can take to protect their systems.

In 2019, CISA initiated and now leads a monthly ***Resilient Power Working Group (RPWG) with over 80 members from the private sector and federal, state and local, tribal, and territorial governments.*** The RPWG is developing the Resilient Power Guidelines, which will be used to support EMP mitigation planning and pilots.

One such pilot is the San Antonio Electromagnetic Defense Initiative, designed to show ***how an entire region can become resilient against an EMP.*** These pilots are multisector, multifunction efforts, seeking to ensure key capabilities continue to function in a post EMP environment and that by maintaining those key functions we can expedite a full recovery.

Recognizing that EMP presents a strategic threat to the nation, ***DHS continues to plan and execute*** on the President's and Congress's intent of sustainable, efficient, and cost-effective approaches to EMP mitigation.

In the last year, the ***Department has made great progress and this work will continue***—with a particular focus on partnership with industry in hardening critical infrastructure—in the next year and beyond".

"*In the last year, the Department has made great progress*" - we read in this report. "Great progress"? In what aspects? Are the USA power systems more protected from HEMP now? Or did they find any fresh data about such a new and unstudied field over the last 50 years phenomenon, or its impact on electrical equipment? …and this work will continue…? What kind of works? Like reading reports yellowed with age?

In the same year (2019), another report "High-Altitude Electromagnetic Pulse and the Bulk Power System Potential Impacts and Mitigation Strategy" prepared by the world-renowned research center EPRI was published.

That report called into question the overestimated danger of HEMP and stated that HEMP is dangerous for limited types of equipment, such as for power transformers. And all hell broke loose! EPRI received a barrage of insults, see Fig. 1.8.

HEMP evangelists applied a bunch of vibrant epithets to unfortunate EPRI: they called the report "detractors", "old-time snake oil", "junk science", etc. All those feedbacks were virtually saturated with the fear to lose the funds spent on their endless "R & D to better understand".

Fig. 1.8. Offensive headlines of some critical publications regarding EPRI report on US media.

However, 2019 was an even more eventful year for HEMP experts — that year a new working group of CIGRE (International Council on Large Electric Systems) was meant to start the work, see Fig. 1.9.

cigre

CIGRE Study Committee C4

PROPOSAL FOR THE CREATION OF A NEW WORKING GROUP[1]

WG N° C4.54	**Name of Convenor:** William Radasky (USA) **E-mail address:** wradasky@aol.com
Strategic Directions #[2]: 1	**Technical Issues #[3]: 6**
The WG applies to distribution networks[4]: Yes	
Potential Benefit of WG work #[6]: 1, 2 and 3	
Title of the Group: Protection of high voltage power network control electronics from the High-altitude Electromagnetic pulse (HEMP)	

cigre

☒ Electra report ☒ Tutorial[5]	
Time Schedule: start: January 2019	**Final Report**: December 2022
Approval by Technical Committee Chairman: **Date**: November 16th, 2018	

Fig. 1.9. Document for registration of new WG C4.54 CIGRE "Protection of High Voltage Power Network Control Electronics from the High-Altitude Electromagnetic Pulse (HEMP)"

What? Has the well-established organization finally decided to deal with this important challenge? No way. I was invited to participate in that research group and offered the results of my tests and researches. However, they immediately said to me: no new researches and no new tests. The task of the group was to summarize the previous publications on that subject and to prepare a report. That was it! It appeared that no one cared about my practical researches and recommendations. No one wanted to understand what that was about. Here, it is worth mentioning that several years ago all those "summarizations of previous works" have been "summarized" in a report "Protection of high voltage power network control electronics against Intentional Electromagnetic Interference (IEMI)" of WG C4.206 CIGRE, headed by the same convener.

As a former member of that working group, I understood that the basic task of WG C4.54 CIGRE was to conduct numerous meetings at nice and beautiful places all over the world – from China to the USA. Unfortunately, all those excellent plans were disrupted by COVID-19, and the group have not published any report.

Fig. 1.10. The new SEL-400G digital protection system, concentrated in a single module all protection functions of power station generator; all protection functions of bus bar and all protection functions of step-up power transformer.

In Russia, the situation is substantially different. Only several major militaries and civil (however, funded by the military) research centers deal with this problem, such as: "The 12th Central Scientific Research Institute" (military unit 51105, town Sergiyev Posad), All-Russian Scientific Research Institute for Experimental Physics - VNIIEF (town Sarov), All-Russian Scientific Research Institute of Technical Physics – VNIITF (town Snezhinsk), Joint Institute for High Temperatures of Russian Academy of Sciences - IVTAN (Moscow). While in Russia no private companies are realizing a profit from HEMP researches, the employees of military and state organizations, in the same way as in the USA, are directly interested in maintaining funding levels and thus keeping the status quo, and do not want to quickly solve the problems. However, there is a difference. While they want to keep the high funding, they are interested in doing as few real things as possible, and hold minimum responsibility for the results and status of this sector in the country. Thus, in contrast to the USA, most works on this subject are classified and the HEMP problem is de facto considered off-limits by public media. As a result, it is difficult to find a power industry expert familiar with this problem. In Russia, attempts to publish a technical article on this topic in a technical magazine specialized in electric power

issues often barge into the opposition of reviewers who do not understand the subject at all, and write outright nonsense in their reviews demonstrating their complete incompetence in this field. And this situation has persisted for decades.

In the meantime, the situation continues to worsen. The concentration of not only all protective functions in one single digital protection relay continues, but also the protection of a whole group of important energy objects in single protection relay, Fig. 1.10. If such single module will damage due to HEMP impact, all power equipment of the power plant will remain unprotected (in the best case) or will be damaged due to improper actions and commands of this protection relay (in the worst case).

In parallel, the development and implementation of artificial intelligence systems in the electric power industry continues, Fig. 1.11, without any limitations and without regard to the increasing significantly vulnerability of the electric power industry to HEMP with such development trends.

Fig. 1.11. Article in a journal "Protection, Automation and Control World", September 2020, p. 28.

While preparing the book: "Protecting Electrical Equipment. New Practices for Preventing High Altitude Electromagnetic Pulse Impacts" for publication, I asked many experts who knew about my monograph: "Protecting Electrical Equipment. New Practices for Preventing High Altitude Electromagnetic Pulse Impacts" to give their comments and received one and only one feedback from Dr. Alexander Prishchepenko, a well-known Russian expert in EMP-ammo development.

Why did other experts refuse to assess the book? It is clear - because my books preclude them from profiting financially!

And here is a list of journals to which I sent for publication my critical article on the state of affairs with infrastructure protection:

- Homeland Defense & Security Information Analysis Center (HDIAC);
- Mission Critical (Data center and mission-critical facility solutions);
- National Defense Magazine;
- Homeland Security Today;

- Interference Technology;
- Domestic Preparedness;
- In Compliance Magazine;
- The Simon Center.

All of these organizations have published articles about HEMP, and so I invited them to publish my article. But the editors of these magazines did not want to answer me at all, even after repeated reminders!

Isn't it strange? Doesn't that say anything?

Chapter II

Cybernetic and Electromagnetic Impacts on Electronic Equipment: Do they Have Anything in Common?

The issue of combining "cyber impacts" and "electromagnetic impacts" into a common concept eventually results in logical combination of potential threats and practical combination of efforts to prevent them and ensure protection against them. In these circumstances, some agencies and specialists aim to develop measures which ensure protection from both cybernetic and electromagnetic threats. Are these threats really so close that some agencies and specialists can successfully address them? Let us examine this issue.

Let us start with cyberspace. Initially this concept was introduced by American writer William Ford **Gibson in his science fiction novel** *Neuromancer* [2.1], Fig. 2.1.

Fig. 2.1. William Gibson and the cover of the first printing of Neuromancer (1984) [2.1].

Today, though the concept has no common definition, it is widely spread in society. There are dozens of absolutely different definitions, from:

"Cyberspace – amorphous, supposedly "virtual" world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet's infrastructure" (Encyclopedia Britannica)
to the definition of the US Department of Defense [2.2], Fig. 2.2:

"Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

In other words, it refers to electronic equipment processing information and computer software installed in this equipment.

The Allied Joint Doctrine for Information Operations NATO AJP-3.10 [2.3] (Fig. 2.2) provides the following definition of "information environment":

"Information environment – the virtual and physical space in which information is received, processed and conveyed. It consists of the information itself and information systems."

In this definition, "physical space" means electronic (computer) equipment, whereas "virtual space" means software environment. Joint work of both environments ensures reception, processing and conveying of information.
However, let us leave fierce philosophic debates regarding "cyberspace" definitions and continue. What is important for us is that this concerns two components of common the **information environment:** electromagnetic range (where information is physically processed by a computer) and virtual space (where information is processed by software). It should be stressed again: it is all about operations in the **information environment** and not elsewhere!

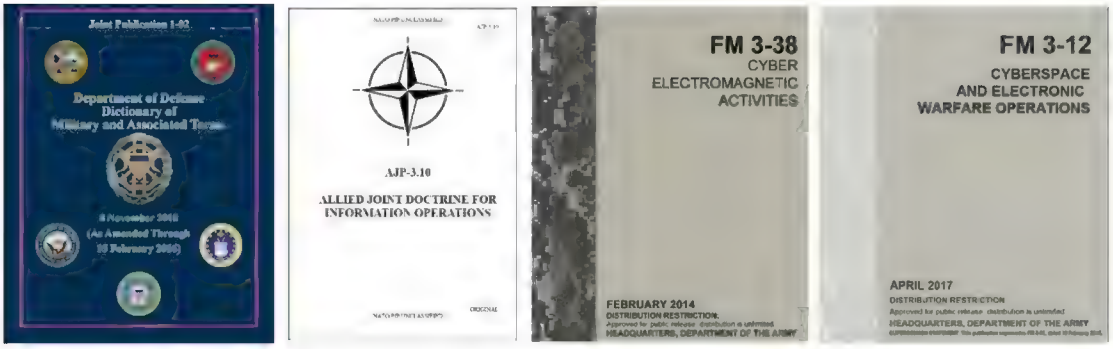


Fig. 2.2. Documents of NATO and US Army regarding cyberspace and electromagnetic impacts.

Operations in cyberspace are divided into several major types, which include multiple sub-types:

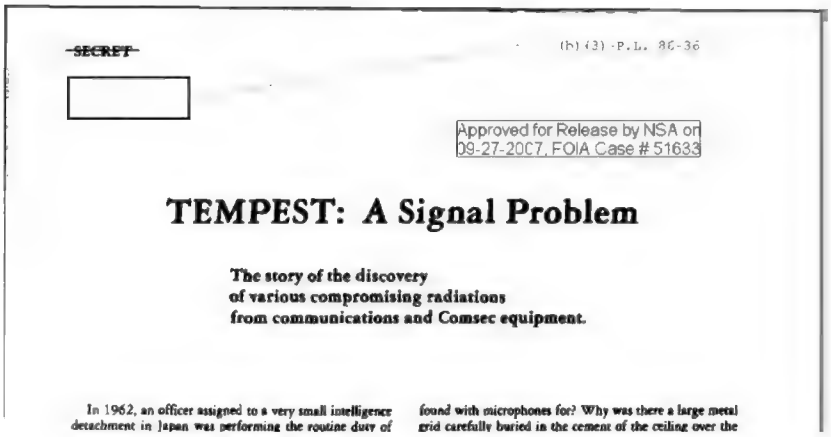
1. Data theft (information leak) by means of special software.
2. Intentional failures of equipment induced by special software.
3. Creation of fake data by fraudulent systems (fishing, clickjacking, information traps, etc.) operating on the basis of special software.

These types of cyberspace operations are based on a common technique (method) of using special software, which intrudes into computers that process information. Thus, joining them into a common concept of "cyber activity" is rather evident and justified.

Operations in the electromagnetic range also consist of several major types which include sub-types:

1. Data theft (information leak) by means of specific highly unusual electronic equipment. Back in 1960s the US National Security Agency (NSA) gave a code name to this technology – "TEMPEST" – and everything related to this topic was classified for dozens of years (Fig. 2.3).
2. Intentional failures of equipment induced by a powerful directed electromagnetic emission with a local impact.
3. Creation of fake data and images by fraudulent systems which produce long-ranging powerful electromagnetic fields that deceive recognition and navigation electronic systems (spoofing, electromagnetic traps, fake targets).

4. Comprehensive and spacious physical damage of different electrotechnical and electronic (not only informational) equipment (electromagnetic pulse of high-altitude nuclear explosion - HEMP).



~~SECRET~~

(b)(3)-P.L. 86-36

Approved for Release by NSA on 09-27-2007, FOIA Case # 51633

TEMPEST: A Signal Problem

The story of the discovery
of various compromising radiations
from communications and Comsec equipment.

In 1962, an officer assigned to a very small intelligence detachment in Japan was performing the routine duty of

found with microphones for? Why was there a large metal grid carefully buried in the cement of the ceiling over the

Fig.2.3. One of the documents from 1960s regarding TEMPEST was declassified by NSA in 2007.

DEPARTMENT OF THE ARMY
U.S. Army Corps of Engineers
Washington, DC 20314-1000

EP 1110-3-2

CEMP-ET

Pamphlet
No. 1110-3-2

31 December 1990

Engineering and Design
ELECTROMAGNETIC PULSE (EMP) AND TEMPEST PROTECTION FOR FACILITIES

1. Purpose. This pamphlet provides unclassified engineering and design information about protecting fixed ground facilities against the effects of an electromagnetic pulse (EMP) produced by a nuclear explosion. It also provides unclassified engineering and design information about satisfying TEMPEST requirements.

2. Applicability. This pamphlet applies to all HQUSACE/OCE elements, major subordinate commands, districts, laboratories, and field operating activities (FOA) having military construction and design responsibilities.

3. Discussion. The enclosed material constitutes a general reference work on the specialized subject of electromagnetic pulse (EMP) and TEMPEST protection. It was assembled over several years by our Construction Engineering Research Laboratory. The designer who is interested in the theory behind the-design will find this material useful. The designer will also find information on aspects of the subject not normally part of the design effort.

FOR THE COMMANDER:

ROBERT L. HERNDON
Colonel, Corps of Engineers
Chief of Staff

Encl

Fig. 2. 4. Cover page of US Army's report # EP 1110-3-2, which combines absolutely different types of activity in the electromagnetic range, i.e. HEMP and TEMPEST [2.4].

Unlike cyberspace operations, those performed in the electromagnetic range have no common grounds (technique, methodology). They differ from each other significantly and thus combining them into a common concept of "electromagnetic activity" is not feasible. For example, what is common between ultra-sensitive sensors of the electromagnetic field used for information retrieval from communication cables (TEMPEST), powerful generators of electromagnetic field with a frequency of dozens of gigahertz, and power rating of several million Watts in a directional antenna and nuclear explosion at the height of several hundreds of kilometers?

Table 2.1. Differences between TEMPEST and HEMP:

Differences	
TEMPEST	**HEMP**
SIGNALS POWER	
MICROVOLTS, MICROWATS	KILOVOLTS, MEGAWATS
FREQUENCY MARGIN	
UP TO 100 GHz	UP TO 100 MHz
MAIN PROTECTION MEASURES	
EMI FILTERS	VOLTAGE SUPPRESSORS
AREA OF USAGE	
LOCAL INSTALLATION	GLOBAL IMPACT
IMPACT ON CRITICAL INSTALLATION	
UNAUTHORIZED ACCESS TO CLASSIFIED INFORMATION	PHYSICAL DESTRUCTION OF INFRASTRUCTURAL OBJECTS
TESTING METHOD AND TEST EQUIPMENT	
VERY HIGHLY SENSITIVE COMPACT ELECTRONIC EQUIPMENT	VERY HIGH-POWER HIGH VOLTAGE BIG EQUIPMENT

However, 30 years ago the US Army Corps of Engineers compiled a substantial report about the results of an Engineer Research Lab operation, where an attempt was made to combine different types of activity in the electromagnetic range, taking HEMP and TEMPEST as an example [2.4] (Fig. 2.4). This combination is very strange due to significant differences between these types of activity in the electromagnetic range (Table 2.1).

Indeed, there is nothing common between these two types of activity, except for shielding requirements for equipment and cables.

Nevertheless, close connection between the electromagnetic range and virtual space in the information environment, as well as some logical similarity of selected operations both in cyberspace and the electromagnetic range, initiated an official introduction of a new concept: "cyber-electromagnetic activity", which would combine both types of activity into a single whole. The reasoning of authors of this concept is not clear, as the notion of cyberspace already includes electronic equipment working in the electromagnetic range. Introduction of a new concept would have been feasible if cyberspace included only the virtual space (i.e. software) and did not include physical processes of information processing by means of electronic equipment. But this is not the case.

Subsequently, how is this relatively new concept used in practice? Let us review some documents of the US Army (Fig. 2.2). The authors of FM 3-38 (2014) (Fig. 2.2) [2.5], which pretends to be the first in creation of a new military doctrine called "*Cyber-Electromagnetic Activities" (CEMA),* suggest a necessity to "integrate and synchronize" operations in cyberspace and the electromagnetic range. One of the examples of such "integration and synchronization" has been discussed above based on US Army report # 1110-3-2.

In the attempt to follow a fashionable doctrine, the Department of Homeland Security (DHS) established the National Cybersecurity and Communication Integration Center (NCCIC), the purpose of which is to coordinate efforts in the field of cybersecurity, protection from HEMP, high-frequency directional electromagnetic weapons, and even from electromagnetic storms during solar flares.

Fig. 2.5. The document containing suggestions on how to prepare critical infrastructure to "cyber-electromagnetic pulse" attacks [2.8].

The attempts to combine absolutely different (in physical essence) impacts on equipment give rise to really "strange" documents, such as the one shown in Fig. 2.5.
Another one is FM 3-12 [2.7] (Fig. 2.2), connecting cyberspace operations with HEMP, which are not associated with cyberspace, without addressing the TEMPEST problem, which should really be combined with cyberspace operations as one of the two components of a common problem of information protection.

Conclusions

1. Various operations in cyberspace have very much in common. Thus, it is rather logical and feasible to combine them into a common group of operations performed in the information environment.
2. Various operations in the electromagnetic range may significantly differ from each other. Moreover, not all of them are associated with the information environment.
3. The concept of cyber-electromagnetic activity covers only those operations performed in the electromagnetic range that relate to the information environment, i.e. the environment, where cyberactivity actually takes place.
4. It is not really feasible to combine absolutely different concepts, one of which relates to the information environment and the other which is not connected (e.g. Cyberactivity and HEMP) automatically. This results in confusion and incorrect allocation of efforts and resources aimed at protection from the destructive impact on critical electronic equipment and thus, this malpractice should be seized.

References

[2.1] Gibson, William. Neuromancer. ACE, July 1984.
[2.2] JP 1-02 Department of Defense Dictionary of Military and Associated Terms. 2010.
[2.3] AJP-3.10 Allied Joint Doctrine for Information Operations. NATO Standardization Agency,
2009.
[2.4] EP1110-3-2 Engineering and Design Electromagnetic Pulse (EMP) and TEMPEST Protection for Facilities. Department of the Army, U.S. Army Corps of Engineers, 1990.
[2.5] FM 3-38 Cyber Electromagnetic Activities. - Headquarters, Department of the Army, 2014.
[2.6] Winks D. Preparing Critical Infrastructure for a Cyber-Electromagnetic Pulse Attack, AcquSight, GSX Infragard, 2018.
[2.7] FM 3-12 Cyberspace and Electronic Warfare Operations - Headquarters, Department of the Army, 2017.

CHAPTER III

Costly Fakes and Reality

"... should not wait for the federal government to take action, we need to take action now to protect our portion of the grid."
David Gregory,
Chairman of the Special Committee on Government Accountability,
member of the Missouri House of Representatives

The ability of the powerful electromagnetic pulse, generated upon the nuclear explosion (HEMP) to destroy all electronics, has been known to nuclear physicists since the first nuclear explosion was performed in 1945 on the Alamogordo range, New Mexico (project Trinity). Upon the explosion, all apparatus that was meant to monitor the explosion parameters became inoperative. Upon all further test explosions performed in all countries, that electromagnetic pulse was registered precisely and was followed with the analysis and study of the parameters. Beginning in the 1970s (50 years ago), that subject has been unclassified. At that time, dozens of Western scientific and technical reports, prepared by numerous military and civilian organizations (working at the military request), were devoted to different aspects of HEMP impact on electrical equipment and electronics. Since then, the electromagnetic pulse had been officially recognized as one of the damage effects of nuclear weapons, along with the detonation wave, the temperature, the light and the radioactive emission. This has been mentioned in all open sources, including booklets and recommendations on protection against the massive weapons distributed amongst the population during the "cold war" between the USA and the USSR. However, at that time only a few people understood. Unfortunately, the situation has not changed a lot, despite hundreds of reports, presentations, articles and books, as well as dozens of open military and civilian standards on this subject. At least in the USA, this subject is in the spotlight of many dozens of organizations listed in [3.1], including numerous Congress Panels created especially for this. Many years have been spent researching this subject which has been funded prevalently by the government. However, civil engineers working in the field of electrical power supply, water supply, sewage systems, telecommunication, banking, etc., are bewildered about this massive data so far. Why? The following is written in the [3.2]:

> *"There are many misconceptions about EMP that are circulating among both technical and policy experts, in press reports, on preparedness websites, and even embedded in technical journals. Because many aspects of the EMP fields and system interaction physics are non-intuitive, misconceptions are inevitable. Uneasiness about the wide-area, ubiquitous effects of EMP and the diversity of systems affected make it convenient to adopt misconceptions that avoid the need for action. Denying the seriousness of the effect appears perfectly responsible to many stakeholder groups. Misconceptions involving consequence minimization or hyperbole have served to deter action in the past. Downplaying the threats places EMP preparedness on the back-burner compared to other effects. Exaggeration of the threats causes policy-makers to dismiss arguments, ascribing them to tin foil hat conspiracy theories."*

The problem is that all such numerous organizations which are fed on massaging the HEMP issue and periodically frightening the laymen with a fatal disaster resulting from the HEMP impact are not interested in an early solution to this issue and are discontinuing research.

Conversely, they are all interested in keeping this problem afloat and continuation of prolonged funding. They endeavor to put aside simple and effective solutions to many technical issues.

Author learned it first hand when he attempted to contact one of the US officials dealing with this subject. When the official mentioned the very important and not yet settled question of protection of a power transformer against HEMP, author answered that in fact he can offer a simple, cheap and field-proven technical solution. The official immediately rebuffed author and did not even ask about the solution.

Also, even people devoted to solve the problem do not understand it clearly. When author sent a promotional brochure of its new book about technical means of HEMP protection to one of the leading HEMP protection actors in the USA, the former chairman of one of the Congress Commissions, author received an amazing answer. It stated that all engineers working in the field of protection of equipment against HEMP do not understand the nature of the problem. In his opinion, it does not require any technical advancements (since all technical issues, according to him, have been solved for some time by the military), rather it requires the attention of the government and society. Subsequently, he proposed to stop wasting time (i.e. stop looking for the technical solutions) and join our forces to react on society. When author tried to explain that military technical solutions are not appropriate for the civilian sector and we need to find new solutions from scratch, it became obvious that he did not understand me and adhered to his opinion that all technical problems were solved long ago.

The opinion that all technical problems have long been solved by the military and one just needs to use their solutions and their experience in the civilian sector can be heard often. Here is what Dr. George H. Baker, Prof. Emeritus James Madison University, Director Foundation for Resilient Societies says in his testimony before the Senate Homeland Security Committeein of Congress [3.3]:

> *"The U.S. military already has EMP protection approaches that are practical, affordable, tested and well understood that can be translated directly to electric power grid control facilities and supervisory control and data acquisition electronics and networks."*

In his numerous publications Dr. Peter Vincent Pry, Executive Director of the Task Force on National and Homeland Security has said the same thing many times:

> *"The problem is not the technology. We know how to protect against it. It's not the money, it doesn't cost that much. The problem is the politics. It always seems to be the politics that gets in the way".*

The same idea, but in different words, is repeated by Ambassador Henry F. Cooper, Chairman of High Frontier, and an acknowledged expert on strategic and space national security issues [3.4]:

> *"Moreover, I emphasized that we have the technical know-how to accomplish this objective; actually, have known how for decades but have not done so for political — not technical or financial reasons".*

The leading research centers also contribute to the creation of such a distorted view of this problem, publishing advertisements about their developments as a panacea for all the ills associated with HEMP, as a unique solution, after which one can do nothing more and to simply rest on our laurels, Fig. 3.1.

Compare these advertisements posted on dozens of websites:

"20 kV Gallium Nitride pn Diode Electro-Magnetic Pulse Arrestor for Grid Reliability
Sandia National Laboratories will develop a new device to prevent EMP damage to the power grid. The EMP arrestor will be comprised of diodes fabricated from the semiconductor gallium nitride (GaN), capable of responding on the ns timescale required to protect the grid against EMP threats. The diodes will be capable of blocking 20 kilovolts (kV), enabling a single device to protect distribution-level equipment on the grid. The team will focus on the epitaxial crystal growth of GaN layers and device design needed to achieve the 20 kV performance target."

"Record-Breaking, Ultrafast Devices Step to Protecting the Grid from EMPs
Scientists from Sandia National Laboratories have announced a tiny, electronic device that can shunt excess electricity within a few billionths of a second while operating at a record-breaking 6,400 volts — a significant step towards protecting the nation's electric grid from an electromagnetic pulse."

Fig. 3.1. One of the fakes spread by Sandia National Laboratories (SNL) that their microscopic element is a revolution in technology and now you can "sleep well": a national electric grid is protected well against HEMP.

and compare with real achievements:

"Demonstration of >6.0-kV Breakdown Voltage in Large Area Vertical GaN p-n Diodes with Step-Etched Junction Termination Extensions

Vertical gallium nitride (GaN) p-n diodes have garnered significant interest for use in power electronics where high-voltage blocking and high-power efficiency are of concern. In this article, we detail the growth and fabrication methods used to develop a large area (1 mm^2) vertical GaN p-n diode capable of a 6.0-kV breakdown. We also demonstrate a large area diode with a forward pulsed current of 3.5 A, an 8.3- $m\Omega \cdot cm^2$ differential specific ON-resistance, and a 5.3-kV reverse breakdown. In addition, we report on a smaller area diode (0.063 mm^2) that is capable of 6.4-kV breakdown with a differential specific ON-resistance of 10.2 $m\Omega \cdot cm^2$, when accounting for current spreading through the drift region at a 45° angle. Finally, the demonstration of avalanche breakdown is shown for a 0.063-mm^2 diode with a room temperature breakdown of 5.6 kV. These results were achieved via epitaxial growth of a 50-μm drift region with a very low carrier concentration of $<1\times10^{15}$ cm^{-3} and a carefully designed four-zone junction termination extension".

[3.5].

Specifically, in fact, we are referring to a laboratory sample of a semiconductor structure (the so-called "wafer") of a diode (namely, a laboratory structure, and not a final product), based on the well-known Gallium Nitride (GaN) material, from which many types of LEDs are produced, including transistors, diodes. Moreover, we are referring to a structure with an area of only 1 mm2, designed for a short current pulse with an amplitude of only up to 3.5 A, while TVS-diodes are widely represented on the market today with the same time response as the advertised GaN diodes, but for currents of tens of thousands of amperes.

The electrical networks themselves and the powerful equipment of electrical networks are protected by very powerful ZnO varistors with voltages of hundreds of thousands of volts and currents of tens of thousands of amperes. Why was it necessary to mislead the public by presenting laboratory samples completely unsuitable for protecting electrical networks from HEMP? Was it to justify the 6.5 million dollars spent by Sandia National Laboratories to develop another kind of small diode from a well-known material?

An additional way to justify such a cost for developing an electronic component that is not really needed is to declare that the existing well-known and widely used protection component is not effective and is unusable today. In the 102-page report No. SAN2020-11145 entitled "Early-Time (E1) High-Altitude Electromagnetic Pulse Effects on Transient Voltage Surge Suppressors", seven authors try to prove that the existing Transient Voltage Surge Suppressors are unsuitable for protection against HEMP. It emerged that to prove this thesis, all means were good. For example, the authors criticize "Transient Voltage Surge Suppressors" as if they were talking about one type of element. In fact, this term refers to many types of modern protective elements, such as Gas Discharge Tubes (GDT), Metal Oxide Varistor (MOV), avalanche TVS-diodes and many others. All of these have very different properties and characteristics and a different ability to protect against HEMP. When analyzing this report, it transpired that the authors chose MOV for criticism - far from the fastest of the protective elements and they simply ignored the really high-speed elements: avalanche TVS-diodes, which are no worse than those developed by SNL in terms of response time, but at the same time thousands of times more powerful, and mass-produced by various companies (Bourns, Littelfuse, MDE Semiconductor, Eaton, and others), Fig. 3.2.

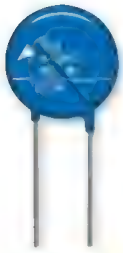
Fig. 3.2. High-power TVS-diodes for peak pulse power up to several megawatts, manufactured by various companies.

The company On Semiconductor back in 2005 published a serious study [3.6], which contains a table comparing the performance data of various types of surge protection devices, Table. 3.1 These data are well known today and this table can even be found in Wikipedia (see article: "Transient voltage suppressor").

Table 3.1. Comparison by the response time (protection time) of Transient Voltage Surge Suppressors of some types [3.6].

Type	Protection Time
GAS TUBE	> 1 µs
MOV	10 – 20 ns
AVALANCHE TVS	50 ps
THYRISTOR TVS	< 3 ns

EPCOS



General technical data

Climatic category	to IEC 60068-1	40/85/56	
Operating temperature	to IEC 61051	−40 ... + 85	°C
Storage temperature		−40 ... +125	°C
Electric strength	to IEC 61051	≥ 2.5	kV_{RMS}
Insulation resistance	to IEC 61051	≥ 100	MΩ
Response time		< 25	ns

BOURNS

Absolute Maximum Ratings (@ T_A = 25 °C Unless Otherwise Noted)

Parameter	Symbol	Min.	Typ.	Max.	Unit
Operating Temperature	T_{OPR}	-40	25	+85	°C
Storage Temperature	T_{STG}	-40	25	+125	°C
Rated Wattage	P_W			1.00	Watt
Varistor Voltage Temperature Coefficient	V_{TC}	0	0.1	0.05	% / °C
Response Time	T_r		10	25	ns
Varistor Voltage Tolerance	V_{tol}	-10	0	10	%

Fig. 3.3. Parameters of some common types of MOV from manufacturer's data sheets.

Nevertheless, it is very interesting how the SNL specialists substantiated their conclusion that the MOV with their reaction time 10 - 20 ns (Fig. 3.3.) are unsuitable for protection against a HEMP (E1) pulse with parameters of 2.5/25 ns.

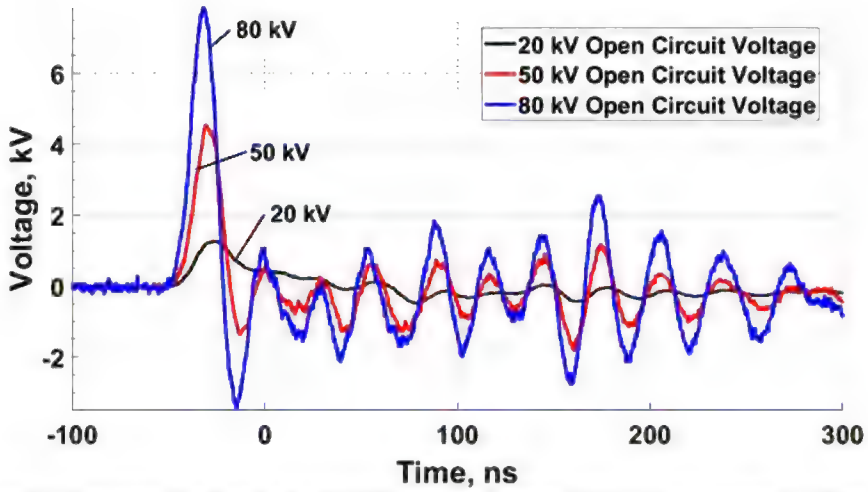


Figure 3-3. Measured Neutral-to-Ground Voltage for Common Mode Configuration of TVSS Test (V3)

The voltage measured throughout the circuit demonstrated a proportional increase as the pulser charge voltage increased. No observable clamping effects were noted which indicates a failure of the TVSS to respond to the insulted pulse. Figure 3-4 – Figure 3-6 demonstrates the response consistency across all devices.

Fig. 3.4a. Oscillograms and comment to them from the SNL report.

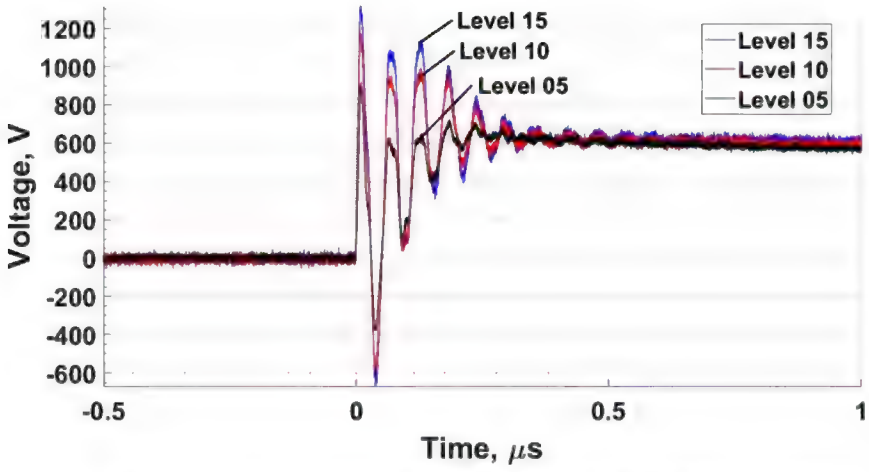


Figure 3-8. Zoomed-In View of Ringing Seen in Clamping Response of TVSS

This clamping time is longer than the duration of the E1 pulse which demonstrates that the TVSSs do not activate quickly enough to respond to it. The response observed in the test is dominated by the capacitance and inductance of the TVSSs.

Fig. 3.4b. Oscillograms and comment to them from the SNL report.

As a consequence: based on such oscillograms, Fig. 3.4, of which there are dozens in the report. It is very interesting how, based on such oscillograms, it is possible to draw conclusions "*that the TVSS do not activate quickly enough to respond to it*"?!

Just amazing!

Today, there are many publications on the reaction time of various types of TVSS in free access. However, the large SNL report (over 100 pages) contains only five literature references, of which three are links to the works of the authors of the report themselves.

If the authors of the report had read numerous publications on this topic, they would have known that the "clamping voltage" of MOV, indicated from the technical documentation, refers to a current not exceeding 100 A. If the current pulse in the experiment had a significantly larger amplitude, then the residual voltage on the MOV will be much higher than the reference value and can reach thousands of volts. Such a high residual voltage has nothing to do with the reaction time.

Additionally, if the authors of the report had read numerous publications on this topic, they would have known that the pulse supplied from the generator to a separate TVSS lying on the laboratory table is completely different from the pulse supplied to the real TVSS placed in the control cabinet, via a cable ten to hundreds of long meters in real operating conditions of equipment in the electric power industry. However, not noticing any difference between laboratory tests and real conditions, the authors extend their conclusion about the unsuitability of MOVs for protecting electrical equipment in substations:

> *"Both common mode and single-ended test configurations demonstrated the TVSS' failure to protect against the E1 pulse. The TVSS' internal MOVs did not respond to the fast pulse due to their activation time... Understanding substation equipment response to the conducted pulses observed in this test due to the failed response of the TVSSs will help determine the level of concern for grid resilience".*

Such publications cause great harm because they mislead specialists.

Moreover, the harm from them is no less than the harm caused from publications of a different kind, proving that allegedly all technical problems have long been resolved. Unfortunately, this is a very common and very dangerous illusion that is replicated by people who are very far from the real technical problems of the civil infrastructure sector. Instead of involving technical experts for solving technical problems, such statements only replicate empty talks and delay the practical solutions of the problem. From this, the pessimism of specialists working in the electric power industry becomes understandable, who directly say that they do not have specific, understandable and affordable means in order to start protecting power energy systems:

> *"Managing that kind of threat right now — no one really has the resources to do that"*
>
> Richard Mroz,
> President of the New Jersey Board of Public Utilities

> "*Much of the available information is not specifically applied to electric utilities, making it very difficult for utilities and regulators to understand effective options for protecting energy infrastructure".*
>
> Robin Manning,
> Vice President for transmission and distribution for the Electric Power Research Institute (EPRI)

It is clear that the more such empty talk and the fewer specific technical solutions suitable for the civilian sector, the longer the problem will remain afloat and the more money can be obtained for this problem.
No less harm and confusion are caused by publications of the opposite meaning, which generally deny the existence of a problem and the need to protect infrastructure from EMP:

EPRI report says existing tech would protect U.S. grid against electromagnetic pulses
"Three years of electromagnetic pulse simulations and testing by the Electric Power Research Institute (EPRI) show that America's electrical grid could withstand the impact of an EMP triggered by a nuclear weapon, according to research findings released on Tuesday by the independent, nonprofit group" [3.7].

Report: Electromagnetic Pulse Would Not Have Widespread Impact on Electric Grid
"EPRI's study found that, while direct exposure to the initial pulse could damage or disrupt some transmission electronics, existing resiliency built into the grid would likely prevent catastrophic failure. Recovery from an EMP would be similar to that from other large-scale power outages, EPRI said" [3.8].

Scientists Are Zapping Fake Electrical Grids to Help Us Survive an EMP Attack
"The results showed that although some parts of power lines and transformer equipment were damaged by the pulses, they weren't as drastically affected as some predictions presumed. And with the control houses, some structures held up better than others — namely the ones made with mostly metal, not concrete. The conductive qualities of metal make the control house act like a Faraday Cage, absorbing and dissipating the incoming energy so none reaches the electronics inside. While the modern-day metal control house designs weren't totally EMP-proof, they did have better shielding qualities than their concrete counterparts" [3.9].

"The Grid Might Survive an Electromagnetic Pulse Just Fine
"A new report enters the debate over whether an EMP from a nuclear blast or a solar flare would cripple the power grid and concludes that actually, we'll probably be OK. Over the past few years, speculation has risen around whether North Korea or any other nation could detonate a nuclear weapon over the United States that would create an electromagnetic pulse and knock out all electricity for weeks or months. This doomsday hypothesis has been promoted by a former CIA director, a commission set up by Congress, and a book by newsman Ted Koppel. But a sober new engineering study by industry experts finds that key equipment on the grid can be protected from any such EMP. Even if it could happen, the resulting blackouts would affect a few states but wouldn't turn the US into a backdrop for **The Walking Dead**.*"* [3.10].

All of these publications refer to the EPRI report, which addresses the issue of the vulnerability of some types of power transformers, and not the entire power electrical grid.

Another sensation. This time from such a serious organization as Department of Homeland Security (DHS):
"*News Release: DHS Releases Recommendations to protect National Public Warning System from EMPs*", Fig. 3.5.

Science and Technology

News Release: DHS Releases Recommendations to Protect National Public Warning System from EMPs

Release Date: September 6, 2022

FOR IMMEDIATE RELEASE

S&T Public Affairs, 202-254-2385

CISA Public Affairs

FEMA Public Affairs

WASHINGTON – Today, the Department of Homeland Security (DHS) released a report of operational approaches to protect the National Public Warning System from an electromagnetic pulse (EMP). The report is a collaborative effort between the DHS Science and Technology Directorate (S&T), the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS) Program, and the Cybersecurity & Infrastructure Security Agency (CISA). The report summarizes recommendations that federal, state, local agencies, and private sector critical infrastructure owners and operators can employ to protect against the effects of an EMP event.

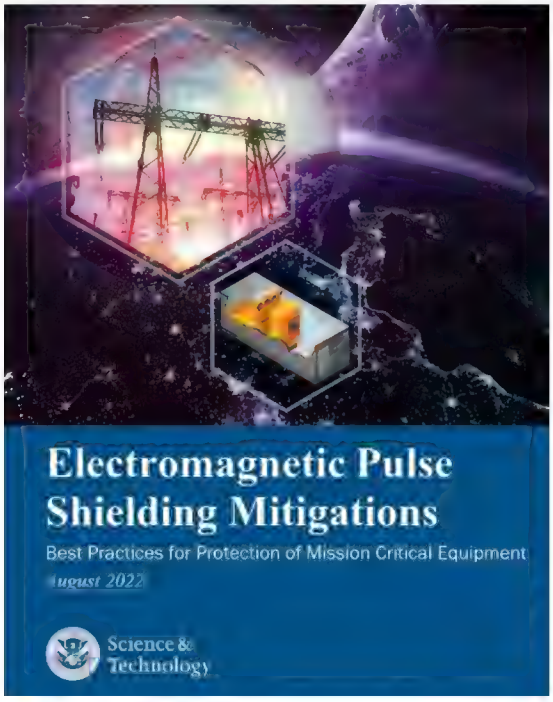


Fig. 3.5a. Promotional publication about the "outstanding achievement" of the DHS Science and Technology Directorate.

Seriously?! Is electromagnetic shielding the new panacea for all EMP problems?! It's a very original achievement of the DHS, Fig. 3.5.

Fig. 3.5b. Promotional publication about the "outstanding achievement" of the DHS Science and Technology Directorate.

It turns out that in order to protect against EMP, it is necessary to shield important equipment and place it in EMP-protected shelters and rooms. What a remarkable discovery nine authors from four government organizations made in their outstanding ten-page report [3.11] that so many media write about!

Such an important discovery must have cost a lot of money to the American treasury... But how could it be otherwise: such important discoveries are usually well paid. In such important matter, DHS does not lag behind SNL…

In fact, as the reader has already guessed, this is a "much of ado about nothing", because the use of metal shells for protection against electromagnetic radiation was proposed by Michael Faraday in 1836. Such protective shells and screens have been widely used in technology for more than 180 years. As for the specific problem of HEMP, this means of protection is discussed in the old articles, reports and standards 30 - 60 years ago [3.12 – 3.18]. In truth, the mountain gave birth to a mouse!

EMP-protected shelters and rooms are widely used in practice to protect military and special governmental installations. Unfortunately, electromagnetic shielding alone, without the use of other means of protection, cannot protect the equipment of power systems and other important infrastructure facilities against EMP. Therefore, next sensation about next "cure for all diseases" should be treated as next fake.

It seems that the topic of EMP and protection against it has become a good "trough" for numerous government organizations. How else can one explain such "outstanding" reports? One would like to ask: aren't you ashamed, gentlemen, for this "olde tyme snake oil"?

It is a serious problem when incompetent journalists begin to disseminate sensational report about the scientific research in the media, without caring about their thorough verification and that they are correctly presented. Alas, here the most important sensation! It doesn't matter if it's correct or not!

One additional problem described in [3.2]:

> *"North American Electrical Reliability Corporation representatives maintain that EMP protection should be addressed by DoD. The DoD points to DHS as responsible for EMP protection of the civilian infrastructure. DHS explains that electric power grid EMP protection belongs DOE since they are the designated Sector Specific Agency (SSA) for the energy infrastructure. EMP protection has become a finger pointing, 'duck-and-cover' game. Our bureaucracy has enabled gaps for addressing the difficult problems of EMP, resulting in no substantive action to protect the nation. We have the classic Washington problem of issues that span departments or fall between departments, which we're all very familiar with, but then we add to that the involvement of the private sector, without central leadership, we're foundering."*

In the field of military technology, no one discusses such topics. All weapons systems are reliably protected from HEMP. But why are they still not suitable for the civilian sector?

There are several very important problems detailed in [3.1, 3.19]. Here are some of them:

Problem 1. Unlike the civilian systems, over the last few decades, all critical military systems vulnerable to HEMP have been designed with HEMP protection. It is much easier and cheaper to include HEMP protection means in the design stage than try to protect the existing critical civilian equipment, such as digital protection relay cabinets used in the power generation industry. Such cabinets, sometimes overstuffed with apparatus, have dozens of inputs and output multicore cables and each separate core requires protection. Who will attend to this?

Problem 2. Internal electrical wiring of military systems (tanks, airplanes, ships, missiles) are made with preassembled wire harnesses or with separate wires in strict adherence to drawings and sizes. Thus, the electrical characteristics of such wiring at high frequencies (HEMP frequencies) are identical to the equipment of the same type. It means that it is sufficient to test the HEMP immunity of one finished typical sample in order to be sure that all other units will have the same characteristics. In the power generation industry, it is hardly possible to find two identical cabinets with electronics having absolutely identical internal wiring. Since at HEMP frequencies range (100 kHz to 100 MHz), the minor change of wire length, even to 20 cm - 30 cm, or in its placement inside the cabinet, results in a dramatic change of cabinet internal apparatus vulnerability to HEMP [3.19], a typical test model does not exist. Thus, the results of testing any individual cabinet for very short electromagnetic pulse impact cannot be extrapolated over other cabinets, i.e., in practice, there is no "typical" cabinet for such tests. Based on conclusions made in [3.1, 3.19], it is not feasible to conduct such tests for this type of equipment.

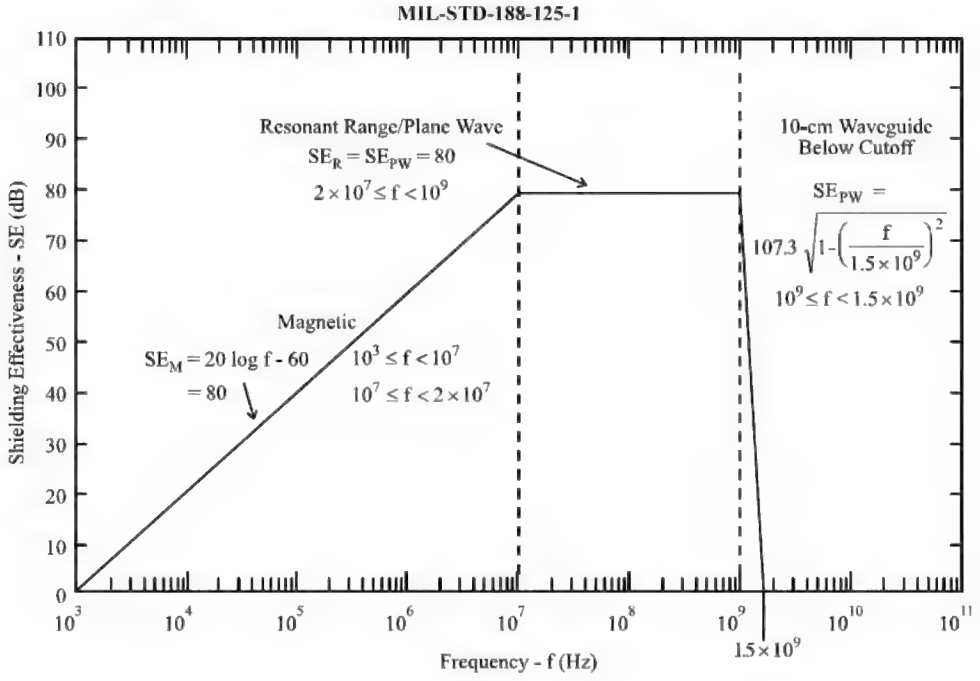


Fig. 3.6. Minimum HEMP shielding effectiveness requirement according to MIL-STD-188-125-1.

The data presented in [3.1] regarding the resilience of computers and computer networks also confirm an extremely large scattering of test results, depending on the influence of a very large number of almost unpredictable factors and the inability to transfer the results of single tests of specific devices and systems to other devices and systems.

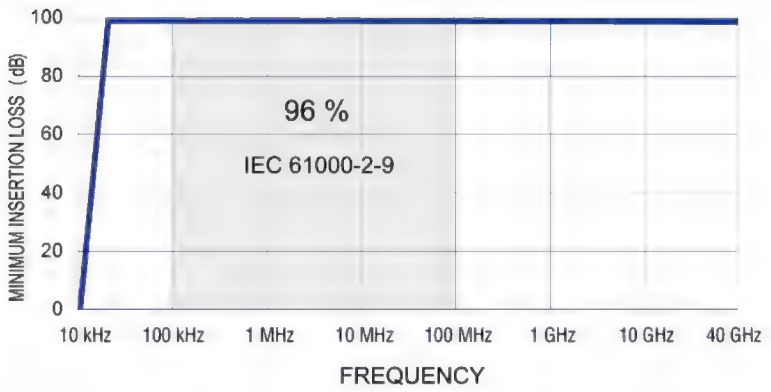


Fig. 3.7. Typical attenuation features of HEMP filters described in ETS-Lindgren's promotion materials.

Problem 3. The military apparatus is protected within the electromagnetic range both from HEMP and Intentional Electromagnetic Interferences (IEMI), as well as from data leak through the electromagnetic fields (TEMPEST). The higher frequency range of IEMI and TEMPEST is far beyond the HEMP range (20 GHz–40 GHz).

Fig. 3.8. HEMP filters installed in a military bunker protected against the nuclear explosion.

However, such means must ensure at least 80 dB – 100 dB attenuation of an electromagnetic interference (signal), Fig. 3.6. Many manufacturers want to be holier than the Pope and offer on the market EMP filters with parameters that exceed the requirements of this standard, Fig. 3.7. The frequency range is allocated in Fig 3.6, in which 96% of the total HEMP energy is released (in accordance with the standard IEC 61000-2-9).

From this it is clear what military protection means, such as electromagnetic filters for electrical circuits of the above-ground electronics in secured bunkers, Fig. 8, which by satisfying such high requirements, will resemble the cabinets with a mass of several dozen kilograms, but will cost several thousand USD each.

Does anyone really believe that civil power engineering can use the same filters simulating the ones used in the underground military bunker? The answer to this question can be obtained from the results of a study carried out by the National Coordinating Center for Communications (USA) [3.20], Table 3.2.

From the presented table, one can see the inexpediency of applying the requirements of military standards to the means of protecting civil equipment. It appears that it is quite enough to attenuate HEMP by 20 - 30 dB only. This significantly changes the attitude towards the problem of protecting civilian equipment.

Table 3.2. HEMP modeling results of damage and upset mitigation for nuclear burst 100 kT at a height of 400 km over the territory of the United States.

Equipment	Protection level, dB	Damage and upset area, sq. km	Damage and upset equipment, %
Ethernet with 30 m cable	0	~5.000.000	69.7
	10	~3.000.000	40.8
	20	~600.000	8.2
	30	0	0
Ordinary telephone system for analog signal transmission over twisted pair (POTS Telephone)	0	~4.000.000	51.5
	10	~900.000	12.9
	20	0	0
	30	0	0
Cordless telephone	0	~6.000.000	78.0
	10	~2.500.000	32.8
	20	~300.000	4.4
	30	0	0

Such a conclusion is also confirmed in [3.21], where it is shown that even for military equipment, the requirements of the basic standard MIL-STD-188-125 [3.17] should not be applied directly to military facilities of all echelons:

> *"If shielding facilities applying the MIL-STD-188-125 standard are installed in all national infrastructures, it is estimated that a huge budget will be required. MIL-STD-188-125 does not consider the blocking and attenuation characteristics of regular buildings or underground facilities in terms of EMP protection. Furthermore, it requires the use of a huge amount of concrete, rebar, and steel plates in heavyweight structures to disallow even a single failure in mission-critical facilities. Hence, there is no need to apply MIL-STD-188-125 to military facilities of all echelons... Therefore, it was confirmed that EMP protection measures could be changed from the current shielding room-oriented, fixed-type protection facilities to mobile lightweight protection facilities using shielding fabrics, shielding racks, redundant equipment, spare equipment, and failure recovery."*

Accordingly, what should be said about civilian equipment?!

Problem 4. This problem is related to the test benches simulating HEMP.
Within such a test bench, such as the guided-wave type HEMP simulator that has been primarily developed for testing pieces of military equipment), the bottom part of the antenna is embedded into a concrete base and has ground potential, Fig. 3.9. It is not a problem for tanks, airplanes, missiles, or other military equipment. However, in the case of civilian equipment, such as cabinets with digital protective relays with grounded internal electronic circuit (i.e. connected

directly to the antenna bottom part), the test bench pulse impact on such a cabinet will differ from the real HEMP, since it will not be related to Earth potential in any way.

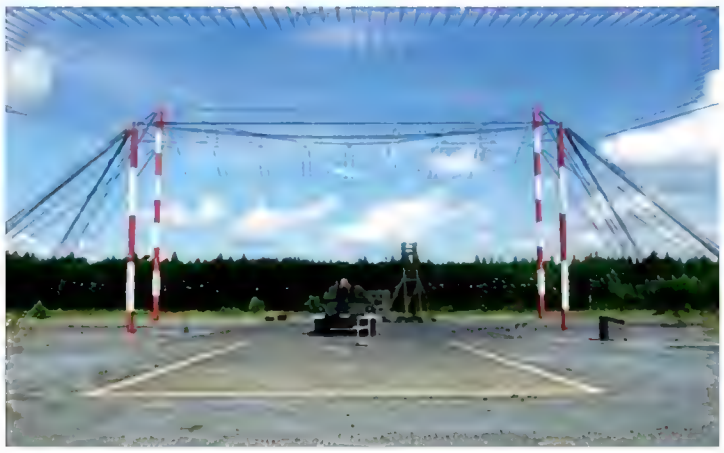


Fig. 3.9. The antenna system of the test bench simulating HEMP.

One other problem of the HEMP simulators. Electronics cabinets used in the power generation industry have dozens of input and output cables, tens and hundreds of meters long. The cables act as antennas absorbing electromagnetic energy over the large area, delivering it directly to the sensitive electronics inside the cabinets. The findings of computer simulation reported by Lawrence Livermore National Laboratory [3.22] suggest that the amplitude on the ends of 45 and 65-meter-long control cables can reach as high as 100-120 kV at an established rating of E1 HEMP's electric field of 50 kV/m. How can such long cables be modeled on a compact test bench? The above image in Fig. 3.9 shows one of the very big benches not available in every country.

As shown in [3.1, 3.19]most existing test benches are of little help for testing cabinet-type equipment, which is used in the civil power industry and the results of these tests are illogical.

Problem 5. Despite a large number of civil and military standards, including the still classified standard [3.23], describing the parameters of HEMP that affect equipment, the real values of these parameters remain completely unpredictable due to objective reasons.

For example, all HEMP-related standards define a field strength of 50 kV/m as a factor affecting the equipment. But in fact, this field strength can be completely different, both much more and much less.

Much more:

> *"On 3 September 2017, immediately after the sixth nuclear test, North Korea claimed that they were capable of attacking with an ultra-powerful EMP by detonating a hydrogen bomb high in the atmosphere"* [3.21].

> *"Russia has "Super-EMP" weapons specialized for HEMP attack that potentially generate 100,000 volts/meter or higher, greatly exceeding the U.S. military hardening standard (50,000 volts/meter)... Super-EMP is a...first-strike weapon," according to Aleksey Vaschenko, who describes Russian nuclear weapons specially designed to make*

extraordinarily powerful HEMP fields as Russia's means for defeating the United States" [3.24].

Much less:

"Through calculations we found that, early-time HEMP has the property of a steep rise time and a slightly slower trailing time; the maximum electric field on ground is located in the area of 1–2 explosion heights to the south of the burst point on the ground; the area of minimum electric field is located at 50 km to the north of the burst point on the ground, about one magnitude smaller than the maximum value, as shown in Table I. This depends upon the inclined angle between the motion trail of the Compton electrons in the transmission direction and the geomagnetic field. If the inclined angle is smaller, the incited Compton currents will be smaller, and the field intensity will be smaller; if the inclined angle is bigger, the field intensity will be bigger" [3.25].

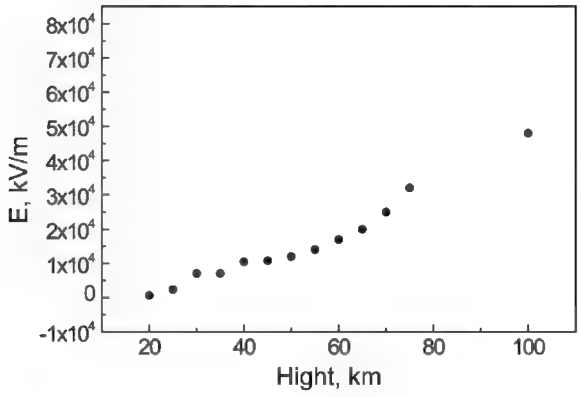


Fig. 3.10. Changes of the electric field intensity at different HOBs over the explosion center for 1Mt yield [3.25].

Table. 3.3 and Fig. 3.10 show only some of the possible variations of the HEMP field strength depending on external conditions, which cannot be predetermined.

There is also a nonlinear relationship between the power of the nuclear charge and the strength of the electric field:

"The power of the 100 kT explosion is 10 times less than that of the 1 MT nuclear explosion, with the electric field intensity peak down by 2.5 times; the power of 500 kT explosion is two times less than that of the 1 MT nuclear explosion, with the field intensity peak down by 15% only" [3.25].

"Due to a limiting atmospheric saturation effect in the EMP generation process, low yield weapons produce peak E1 fields of the same order of magnitude as large yield weapons if they are detonated at altitudes in the 50-80 km range. The advantage of high yield weapons is that their field on the ground is attenuated less significantly at larger heights of burst (that expose larger areas of the Earth's surface)." [3.26].

As can be seen, unpredictable variations in the intensity of HEMP exposure to equipment are possible over a very wide range, Fig. 3.11, 3.12 [3.26].

Table 3.3. Electric field peak value distributed on the ground from a 100 km height of burst (HOB), 1Mt yield burst [3.25].

Location on the ground (Projection point on the ground from the explosion center)	Peak electric field, V/m
50 km to the north	2866
26 to the north	11447
ground zero	20777
57.7 km to the south	35494
100 km to the south	40042
173 km to the south	40227
247 km to the south	37071
290 km to the south	34802
514 km to the south	30796

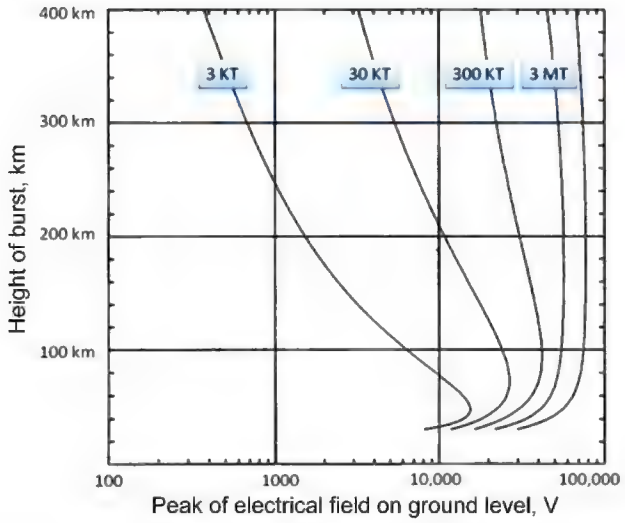


Fig. 3.11. Variations in the intensity of HEMP exposure.

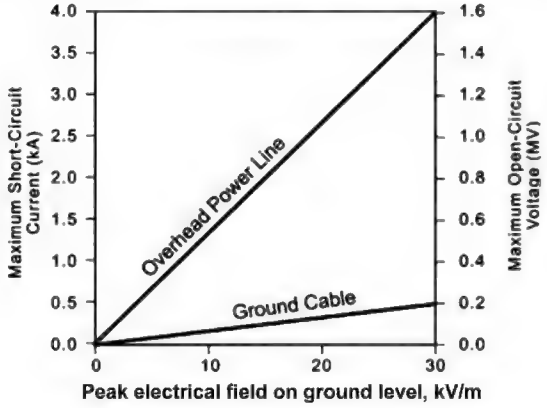


Fig. 3.12. Voltage and current induced in long overhead lines and ground cables by E1component of HEMP from kiloton-class yield weapons.

Problem 6. The next problem is using the requirements of the MIL-STD-188-125-1 [3.17] concerning injection of current pulse at testing resilience of electronic equipment to HEMP.

Table B-I in section B "Pulsed Current Injection (PCI) Test Procedures" of this standard stipulates technical requirements for testing equipment, particularly for a high-voltage pulse generator. This device should generate a current pulse with an amplitude of up to 5,000 A with the source impedance of 60 Ω. According to the standard: "source impedance is the ratio of the generator peak open-circuit voltage to the peak short circuit current", i.e.: $R_{SOURCE} = U_{OPEN}/I_{Sh.C.}$ Thus, the requirement to "open-circuit voltage" can be determined as: $U_{OPEN} = R_{SOURCE} \times I_{Sh.C.} = 60\Omega \times 5{,}000\ A = 300{,}000\ V$. The generator providing such parameters really exist on the market. For example, the Marx type generator, manufactured by Montena EMC company.

In other words, output voltage of the generator, the output terminal which is connected to a circuit with high source impedance, (such as inputs/outputs of low-voltage electronic equipment) can reach as high as hundreds of thousands of volts! Which electronic circuits could sustain this voltage? Why should this voltage be applied to these circuits as they are subject to civil standards [3.27] restricting voltage at 8 kV (level EC8) or 16 kV (level EC9), depending on specific placement of equipment?

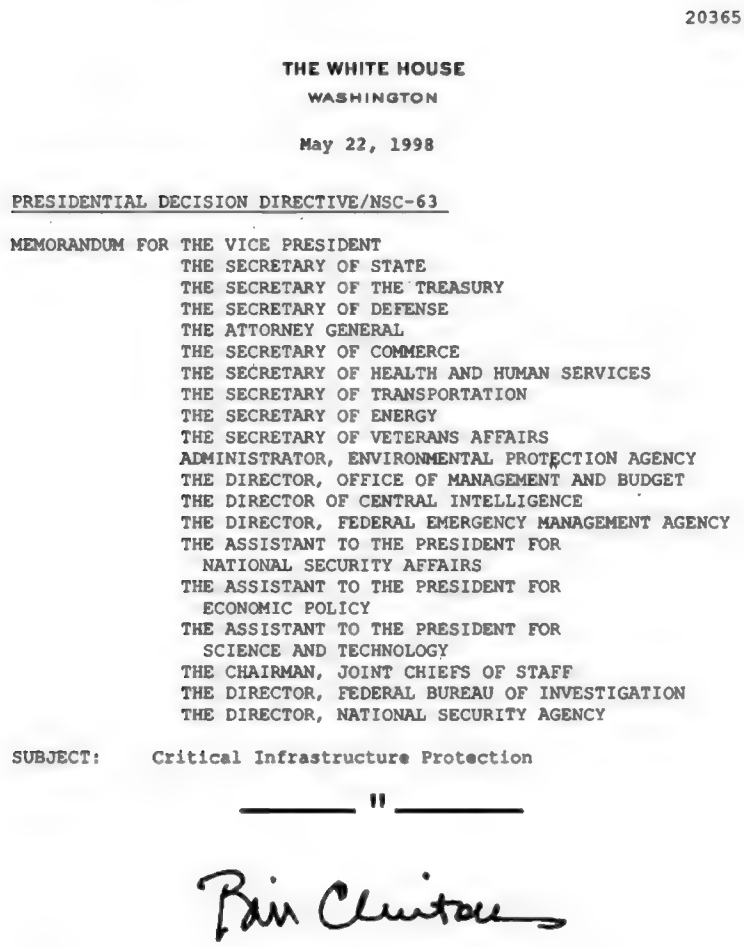
These simple calculations, multiple references in the standard to "conductive circuits" and "short-circuit currents", as well as lack of tests for "differential mode", imply that the requirements of this standard are not applicable for electronic equipment. They are rather suitable for testing of conductive protection devices, such as filters, which are connected into a "common mode", and grounded cable shields. Author assumed this previously [3.1, 3.19] and thus he did not mention pulse current tests as a recommended method of HEMP-resilience testing of electronic equipment. However, some specialist dealing with these tests insists on adhering to requirements of this section of MIL-STD-188-125-1 when testing electronic equipment. It is globally true that HEMP simulators are usually maintained by military men or military industry representatives. These representatives used to work with military standards and often have no idea about existing sets of civil standards. When civil specialists test civil equipment on military test benches, they have no choice but to accept the rules established by the owners of the testing equipment. Hence, a supposed necessity of testing civil equipment based on MIL-STD-188-125-1 is also suggested in various scientific and technical papers. This is the reason why this discussion was necessary to challenge a common opinion.

Consequently, my conclusion is: requirements of section B "Pulsed Current Injection (PCI) Test Procedures" of MIL-STD-188-125-1 are not suitable for testing civil electronic equipment by supplying test pulses to its input and output terminals. Thus, these tests should be excluded from the testing schedule of this equipment to HEMP-resilience. Industrial electronic equipment, meeting the requirements of standards on electromagnetic compatibility, will also be resilient to current pulse flowing through additional input-placed transient suppression protecting elements upon HEMP impact, and thus requires no additional tests to be carried out on special testing equipment stipulated by MIL-STD-188-125-1.

Problem 7. The inability to consider the specific conditions in which thousands of specific types of equipment are located: types of buildings; the location of rooms with interior equipment; the presence of windows; cables, their length, depth in the soil; specific soil properties (which, moreover, change significantly depending on weather conditions), etc. Specifically, the inability to consider the weakening properties of the environment surrounding the equipment in order to assess what additional protective equipment and with what properties are needed. There are thousands of options here.
This raises a very important question regarding assessment of efficiency of applied protection measures and protection means. In this situation I rely on three rationales:

- it is fundamentally impossible to formulate clear technical requirements for HEMP protection of equipment that would be universal for all types of civilian equipment;
- it is impossible to ensure absolute protection for every piece of electronic equipment employed at power facilities;
- any level of protection which can attenuate (at least partially) HEMP impact on electronic equipment is useful.

Based on this, the general strategy should be based on ***maximum use of maximum amount of known protection means with restrictions to be determined by technical and economic capabilities of a specific power system only.***



20365

THE WHITE HOUSE

WASHINGTON

May 22, 1998

PRESIDENTIAL DECISION DIRECTIVE/NSC-63

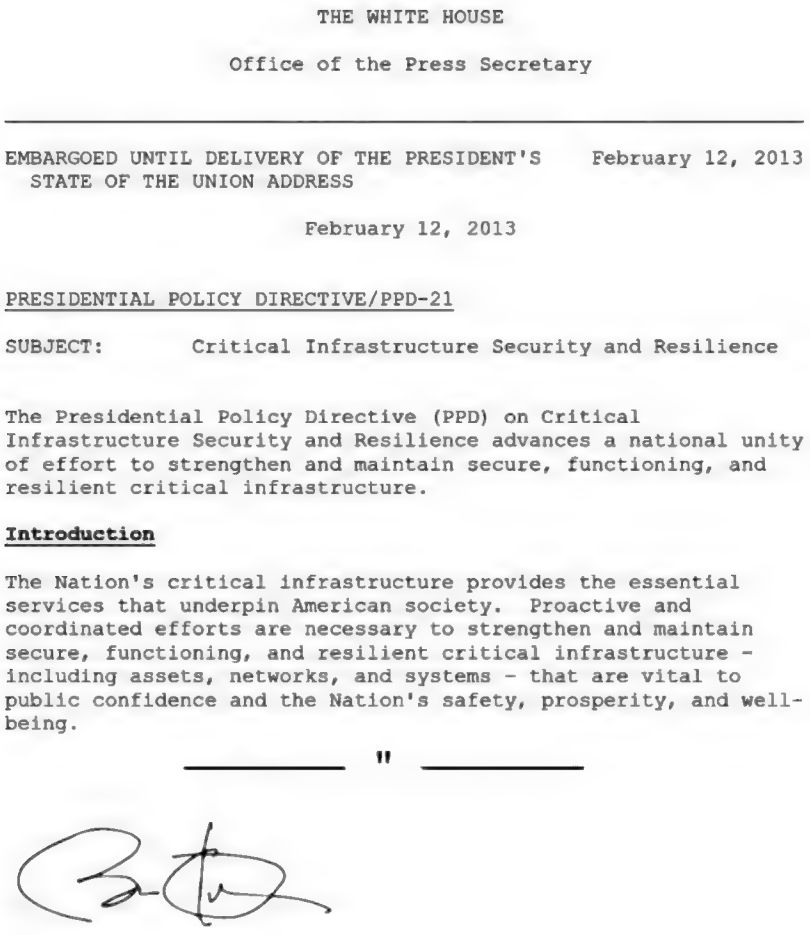
MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF HEALTH AND HUMAN SERVICES
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF ENERGY
THE SECRETARY OF VETERANS AFFAIRS
ADMINISTRATOR, ENVIRONMENTAL PROTECTION AGENCY
THE DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
THE DIRECTOR OF CENTRAL INTELLIGENCE
THE DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY
THE ASSISTANT TO THE PRESIDENT FOR
NATIONAL SECURITY AFFAIRS
THE ASSISTANT TO THE PRESIDENT FOR
ECONOMIC POLICY
THE ASSISTANT TO THE PRESIDENT FOR
SCIENCE AND TECHNOLOGY
THE CHAIRMAN, JOINT CHIEFS OF STAFF
THE DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
THE DIRECTOR, NATIONAL SECURITY AGENCY

SUBJECT: Critical Infrastructure Protection

Fig. 3.13a. Fragment of the first page of the Presidential Decision Directive NSC-63 "Critical Infrastructure Protection", May 22, 1998, signed by former President Bill Clinton.

This approach makes testing of complete protected equipment on simulation test benches absolutely senseless, even if we forget about the downsides of guided wave-type simulators. Nevertheless, some tests are necessary and important. They include testing of specific means (elements) selected for protection, such as varistors, filters, cabinets, cables, etc. The purpose of these tests is to check parameters declared by the manufacturer and to select the most efficient protection elements from the diversity offered in the market. These tests can be performed using generally accessible instruments, manufactured by companies described in [3.1].

All these problems have been detailed in my previous books on this subject [3.1, 3.19].



THE WHITE HOUSE

Office of the Press Secretary

EMBARGOED UNTIL DELIVERY OF THE PRESIDENT'S STATE OF THE UNION ADDRESS — February 12, 2013

February 12, 2013

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

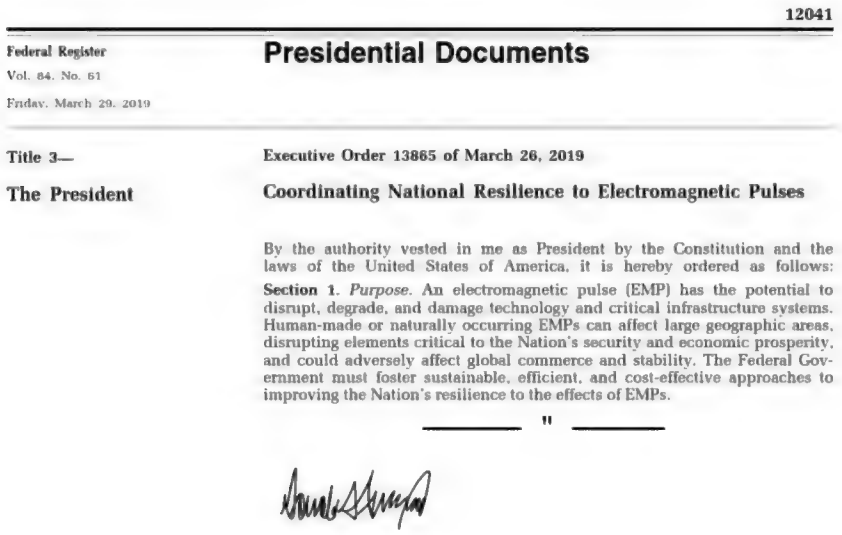
Introduction

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure - including assets, networks, and systems - that are vital to public confidence and the Nation's safety, prosperity, and well-being.

Fig. 3.13b. Fragment of the first page of the Presidential Policy Directive PPD-21 "Critical Infrastructure Security and Resilience", February 12, 2013, signed by former President Barack Obama.

But what is the status in terms of drawing the government's and society's attention to this problem? Just as bad as in terms of technical problems! For many years, the US Presidents have been implementing programs to protect the country's infrastructure, Fig. 3.13, but before President D. Trump there was not even a hint of protection against HEMP (in any event, as if this problem was known at the time). But unfortunately, US bureaucrats and officials have managed to convert the renowned Directive of former President D. Trump "Executive Order on Coordinating National Resilience to Electromagnetic Pulses", into another example of bureaucratic sophistry and verbosity. It was detailed in my previous book [3.19].

As a consequence, nothing essential was done in this regard, and "*the current state of EMP protection is random, disoriented and uncoordinated*", - according to Dr. George H. Baker, Prof. Emeritus James Madison University. Regarding that situation, there is a big range of views amongst different specialists in this field, including the very opposite ones [3.1].



12041

Federal Register
Vol. 84, No. 61
Friday, March 29, 2019

Presidential Documents

Title 3—
The President

Executive Order 13865 of March 26, 2019

Coordinating National Resilience to Electromagnetic Pulses

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Purpose.* An electromagnetic pulse (EMP) has the potential to disrupt, degrade, and damage technology and critical infrastructure systems. Human-made or naturally occurring EMPs can affect large geographic areas, disrupting elements critical to the Nation's security and economic prosperity, and could adversely affect global commerce and stability. The Federal Government must foster sustainable, efficient, and cost-effective approaches to improving the Nation's resilience to the effects of EMPs.

Fig. 3.13c. Fragment of the first page of the Executive Order 13865 "Coordinating National Resilience to Electromagnetic Pulses", March 26, 2019, signed by former President Donald Trump.

For example, Dr. Peter Vincent Pry, Executive Director of the Task Force on National and Homeland Security mentions: "*The problem is not the technology. We know how to protect against it. It's not the money, it doesn't cost that much. The problem is the politics. It always seems to be the politics that gets in the way*". However, other experts take great issue with it. "*I don't think we have an illusion we will prevent it. That's really the government's job*", - says Mike Bryson, Vice President of Operations for the Valley Forge, Pennsylvania-based operator. His words are echoed by another representative of the US electrical energy sector, Richard Mroz, President of the New Jersey Board of Public Utilities: "*Managing that kind of threat right now — no one really has the resources to do that*" [3.1]. General M. V. Hayden, Ex-Director of the National Security Agency (NSA), Ex-Director of the Central Intelligence Agency (CIA) sums up: "*I don't mean to be so flippant, but there really aren't any solutions to THIS, so I would just leave it at that*" [3.1].

"…leave it at that"? Therefore, let us forget and do nothing...Brilliant strategy, isn't it? Nonetheless, the developers of the new weaponry from all countries clearly understand the chosen strategy and the present situation and relentlessly work on the new electromagnetic weapon types, including a super-EMP bomb – a nuclear explosive with a manifold magnification of pulsed electromagnetic radiation, while understanding that there is no protection against it and it will not be available in the near future.

It should be noted here that opponents to any measures on protection of infrastructure against HEMP often say that such protection does not make sense, since any nuclear explosion initiated by any side will immediately result in a massive attack with all nuclear weaponry and a single electromagnetic pulse will be meaningless. In fact, this is not true. Recently, nuclear weapon strategy and tactics have evolved. It is no longer just a strategic deterrent weapon. For example, there are programs on creating new tiny nuclear warheads for tactical cannon shots actively developed in many countries. Here it should be noted that in order to generate a powerful EMP, the nuclear warhead must be activated at a high altitude (more than 30 km), therefore such a warhead is not a mass lethal weapon. This fact should be deemed as an important motivation to apply such weapons. If the weapon will cause no direct human losses, the opponent will hardly

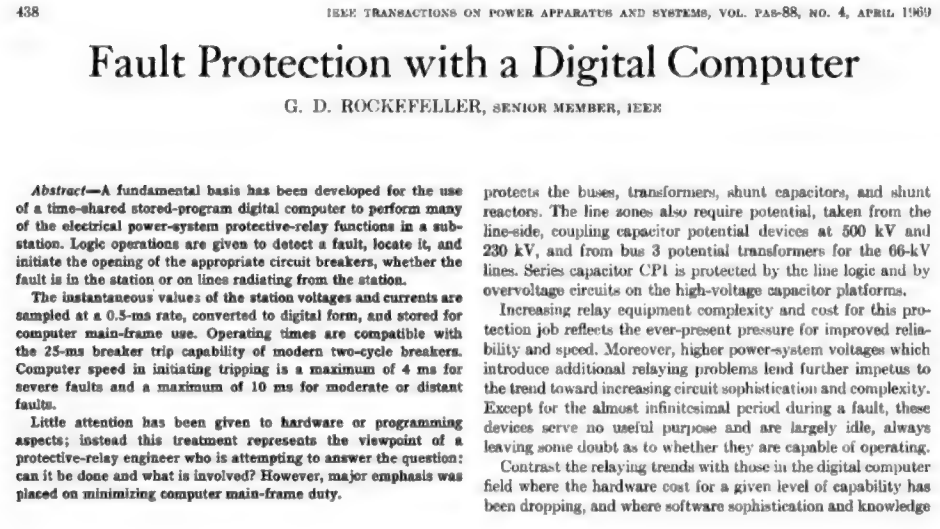
initiate the regular overland nuclear attack resulting in millions of deaths. The response will likely be symmetric. That is why it is very important to protect the infrastructure against HEMP, and this problem will evolve over time.

In his testimony before Senate Committee on Homeland Security, Dr. Peter Pry says [3.28]:

"Today's microelectronics are the foundation of our modern civilization, but are over 1 million times more vulnerable to EMP than the far more primitive and robust electronics of the 1960s, that proved vulnerable during nuclear EMP tests of that era. Tests conducted by the EMP Commission confirmed empirically the theory that, as modern microelectronics become ever smaller and more efficient, and operate ever faster on lower voltages, they also become ever more vulnerable, and can be destroyed or disrupted by much lower EMP field strengths. Microelectronics and electronic systems are everywhere, and run virtually everything in the modern world. All of the civilian critical infrastructures that sustain the economy of the United States, and the lives of 310 million Americans, depend, directly or indirectly, upon electricity and electronic systems.... Another key vulnerability to EMP are Supervisory Control and Data Acquisition systems (SCADAs). SCADAs essentially are small computers, numbering in the millions and ubiquitous everywhere in the critical infrastructures, that perform jobs previously performed by hundreds of thousands of human technicians during the 1960s and before, in the era prior to the microelectronics revolution. SCADAs do things like regulating the flow of electricity into a transformer, controlling the flow of gas through a pipeline, or running traffic control lights. SCADAs enable a few dozen people to run the critical infrastructures for an entire city, whereas previously hundreds or even thousands of technicians were necessary. Unfortunately, SCADAs are especially vulnerable to EMP."

It is related to the expanded application of microelectronics and micro-chips over all technical and technological fields, i.e. to the increased vulnerability of all our lives to HEMP.

In 1969, the American scientist George D. Rockefeller published an article: "Fault protection with a digital computer", Fig. 3.14, in which is considered the beginning of the era of digitalization of relay protection and, in general, the entire electric power industry.



438 IEEE TRANSACTIONS ON POWER APPARATUS AND SYSTEMS, VOL. PAS-88, NO. 4, APRIL 1969

Fault Protection with a Digital Computer

G. D. ROCKEFELLER, SENIOR MEMBER, IEEE

Abstract—A fundamental basis has been developed for the use of a time-shared stored-program digital computer to perform many of the electrical power-system protective-relay functions in a substation. Logic operations are given to detect a fault, locate it, and initiate the opening of the appropriate circuit breakers, whether the fault is in the station or on lines radiating from the station.

The instantaneous values of the station voltages and currents are sampled at a 0.5-ms rate, converted to digital form, and stored for computer main-frame use. Operating times are compatible with the 25-ms breaker trip capability of modern two-cycle breakers. Computer speed in initiating tripping is a maximum of 4 ms for severe faults and a maximum of 10 ms for moderate or distant faults.

Little attention has been given to hardware or programming aspects; instead this treatment represents the viewpoint of a protective-relay engineer who is attempting to answer the question: can it be done and what is involved? However, major emphasis was placed on minimizing computer main-frame duty.

protects the buses, transformers, shunt capacitors, and shunt reactors. The line zones also require potential, taken from the line-side, coupling capacitor potential devices at 500 kV and 230 kV, and from bus 3 potential transformers for the 66-kV lines. Series capacitor CP1 is protected by the line logic and by overvoltage circuits on the high-voltage capacitor platforms.

Increasing relay equipment complexity and cost for this protection job reflects the ever-present pressure for improved reliability and speed. Moreover, higher power-system voltages which introduce additional relaying problems lend further impetus to the trend toward increasing circuit sophistication and complexity. Except for the almost infinitesimal period during a fault, these devices serve no useful purpose and are largely idle, always leaving some doubt as to whether they are capable of operating.

Contrast the relaying trends with those in the digital computer field where the hardware cost for a given level of capability has been dropping, and where software sophistication and knowledge

Fig. 3.14. The first complete publication on the use of a computer in relay protection

Digital protective relays and automatic control systems built on microprocessors, distributed power generation controlled with the artificial intelligence devices, digital substations, etc. All these great and most advanced systems are particularly vulnerable to HEMP.

> "*While this digital transformation has been accepted in our everyday lives and we are all walking around with multifunctional devices in our pockets that function as a phone, TV, radio, GPS receiver, photo camera, videorecorder, etc., for many people in our industry it is a very different story at work. There are still PAC specialists that do not accept the digitization and digitalization of our industry because they prefer to do everything as they always did with the electromechanical devices of the last century, regardless of all the problems they have to deal with... The ones that hesitate to do it are the ones that are going to fail."* - writes the Editor-in-Chief of the popular magazine "Protection, Automation & Control World" (PAC), Alex Apostolov [3.29].

"*...phone, TV, radio, GPS receiver, photo camera, videorecorder in our pockets*" – these are the same as multifunctional relay protection system of power plant or high-voltage transmission system?!!! In my opinion, this is (to put it mildly) not a very smart comparison…

"...specialists that do not accept the digitization and digitalization of our industry because they prefer to do everything as they always did with the electromechanical devices"?! And in my opinion, this is because some experts are used to thinking before deciding, deeply weighing all the pros and cons, not succumbing to general euphoria.

A very dangerous modern phenomenon in the electrical power industry called "digital substation" should be mentioned here. No, of course, it is not dangerous in itself, but in the way it is "implanted" into the power electrical industry. However, no threats stop the digital substation apologists. For them, all ways are good, and possible problems along the way are not even discussed:

"*It was not that long ago when people were asking should we build a digital substation and the answer to this question is already obvious – **yes, we should**"* - say Alex Apostolov, Editor-in-Chief of well-known journal "PAC World" [3.30].

"*Not IF but WHEN*" – this is how the Alex Apostolov, puts the question.

And digital substations begin to march widely across the vastness of the "energy space!", accompanied by resounding advertisements in the technical magazines. Listed below are outstanding features of "digital substations" stated in the such advertisements:

"Reliability – Flexibility – Interoperability

- *40% reduction in maintenance work and outage time*
- *Reduced Footprint, from 10% to 40%*
- *Up to 80% reduction in wire cable*
- *Increased stability and reliability*
- *Low investment and life-cycle cost*
- *Higher efficiency and more safety*
- *Enhanced cyber security"*

Indeed, why not, if they have such outstanding features as stated in the advertisement above?!

Here is just one small feature of a digital substation its apologists are silent about: a sharp increase in the vulnerability of the electrical power industry (and therefore of the entire infrastructure) to intentionally destructive electromagnetic impacts, in particular to HEMP. And author appeals to him with a request to pay attention to this danger that Mr. A. Apostolov simply ignored.

As usual, big businesses are indifferent about the consequences of its activities. Profit is above all!

Especially dangerous is the combination of an unprotected digital substation with the concentration of the basic functions of relay protection in a single module.

The concentration of not only all protective functions in one single digital protection relay continues, but also the protection of a whole group of important energy objects in single protection relay, (SEL-400G, for example, Fig. 1.10, that combined all function of generator, bus and step-up transformer protection). If such a single module will damage due to HEMP impact, all power equipment of the power plant will remain unprotected (in the best case) or will be damaged due to improper actions and commands of this protection relay (in the worst case).

Likewise, as my articles and books are absolutely ignored by companies offering their products in the field of digital substations. Why? It is all very simple [3.31]:

> *"... in 2020 the global business in digital substations was more than 6 billion U. S. dollars with the prediction that this number will go above 9 billion in 2025".*

The development and implementation of artificial intelligence systems in the electric power industry continues without any limitations and without regard to the increasing significantly vulnerability of the electric power industry to HEMP with such development trends. Thus, the modern electrical power industry's development tendency is accompanied by its increasing vulnerability. Is it progress? There is rather a strange situation – while everyone is concerned with the cyber security of today's civil electrical power industry, no one (except me) thinks about its protection against HEMP.

Moreover, author's articles and books inviting the attention to the fast-paced increasing of power systems vulnerability face strong push-back with full rejection and antagonism against its position, including ranting that author try to stop the advancement of the technology. This position of the leading power engineering experts, and all-around appeals to fasten the power engineering sector digitalization by any and all means, without any consideration of the problem or intention to simultaneously develop measures on protection of all those digital technologies against HEMP, are hair-raising.

However, this does not eliminate the need to search for and select the most effective means of protection of the civilian infrastructure from those offered on the market, which have the best price-performance ratio.

Despite the seemingly routine and simplicity of the problem, for a number of reasons this becomes a very difficult task in this specific field of technology. One of the problems is that civilian sectors of the economy have not yet started real work anywhere in the world to protect civilian infrastructure from HEMP, and therefore these sectors are not consumers of protective equipment. For this reason, manufacturers of this protective equipment are primarily focused on

military orders and produce products according to military standards that meet the requirements of the military. As a result, the means of protection offered on the market today have parameters that are excessively high for the needs of civilian infrastructure and, accordingly, a high cost that is completely unacceptable for civilian needs. Specifically, even if in some country, in some sector of the economy, they decide to deal with the problem of protection against HEMP, they will not find anything suitable on the market.

In this regard, the only solution may be to conduct research and development of protective equipment specifically designed for civilian infrastructure with the new strategies and methods for their application. It can be stated that today these tasks have not yet been solved, and numerous reports and recommendations published by dozens of organizations are too vague, not specific, and do not help to solve the problem of protecting civilian infrastructure. They create only a background noise and the illusion that all technical problems have already been resolved and it is only a matter of government decisions.

One example is the report of such a serious organization as the United States Department of Homeland Security [3.32], in the preparation of which more than 10 state organizations took part, such as: US Department of Defense, US Department of Energy, Defense Threat Reduction Agency (DTRA) and many others. This document is relevant because:

> *"Assessments of the risks to civilian critical infrastructure from electromagnetic incidents are intrinsically difficult to produce due to the rarity—or complete absence—of actual events, as well as the fundamental complexity of predicting real-world interactions between electromagnetic pulses and* ***thousands of diverse infrastructure installations****."*

But the strategy and methods for solving this problem are set out in the document in a very wordy and vague way:

- *"Increase coordination..."*
- *"Improve EMP-related intelligence gathering..."*
- *"Review test data on the effects of EMP on critical infrastructure systems that are representative of those currently deployed throughout the Nation..."*
- *"Prioritize new tests of specific infrastructure associated with national critical functions..."*

"Improve EMP-related intelligence gathering..."?! Seriously? And this is after 60 years of research and practical experiments on this phenomenon?!

"*Review test data*" and *"Prioritize new tests"* for "*thousands of diverse infrastructure installations"*?! However, isn't that unintelligent? Especially after it has been proven that among these "*thousands of diverse infrastructure installations*" there are not even two completely identical ones in terms of their high-frequency properties and susceptibility to HEMP.

It is a pity that the authors of the report do not understand that the most important for protection against HEMP parameters of "*thousands of diverse infrastructure installations*", are not determined in fact and any "*EMP-related intelligence gathering"* not will help here.

Moreover, even the parameters of the HEMP itself and the degree of its influence on the infrastructure are uncertain [3.24]. Specifically, in fact, there is complete uncertainty not only of the objects of protection, but also of the impact itself:

> *"Any electric power outage resulting from an EMP event would ultimately depend upon several unknown factors and effects to assets that are challenging to accurately model, making it difficult to provide high-specificity information to electric system planners and system operators. These variables include characteristics such as the EMP device type, the location of the blast, the height of the blast, the yield of the blast and design and operating parameters of the electric power system subject to the blast"* [3.33].

> *"The technical impact of a HEMP event on the electric infrastructure is uncertain... Some proposed the electric industry should install a particular protected device or fully gold-plate the entire grid so that it could survive a HEMP event. However, there's really no consensus on what measures should be taken at this point. The potential unintended effects of that type of protection on the grid or how successful the efforts would be if we, in fact, tried to do that at this time. Cost is a significant factor."* [3.34].

> *"I read the EMP Commission report, I struggled to understand how I could take the plethora of information that was available on EMP and practically apply it to create some sort of a plausible approach for risk management... Certainly impacts from HEMP are real; however, evaluating the effects of such events on complex systems like our electric power grid requires concrete, scientifically-based analysis from people who understand the power system. With greater understanding, cost-effective mitigation and/or recovery options can be developed and deployed."* [3.35].

What is there left to do in such a situation?
And here is what, it turns out, needs to be done in such a situation:

"Disseminate EMP and GMD risk assessment information and research findings with relevant owners and operators of critical infrastructure using existing information-sharing platforms",

as prescribed by the American Strategy [3.32].

Unfortunately, in fact, this is the only task that all such reports solve. But this does not bring us closer to solving the problem of protecting critical infrastructure.

Despite all these problems listed above, serious organizations prefer to simply ignore them. Ultimately, if you notice, then you will need to solve them. It is much easier to issue empty "recommendations" [3.36] that do not bind anyone to anything:

"Recommendations:

- *Develop a long-term comprehensive plan to address the full spectrum of interrelated EM threats*;
- *Employ red-teaming to improve operational planning processes in a way that integrates the full threat spectrum*;
- *Develop and implement EM-specific deterrence policies*;
- *Improve strategic communications to shape perceptions and strengthen deterrence*;
- *Seek incremental hardening and threat-level testing*;
- *Develop an early warning and response system*;

- *Put in place training and processes for smart reconstitution;*
- *Prioritize among protection initiatives based on an analysis of societal functionality;*
- *Establish a political process for prioritization among infrastructure functions;*
- *Use models and experiments to understand society-wide vulnerabilities and responses;*
- *Develop and hold regular national preparedness exercises;*
- *Create insurance mechanisms to mitigate vulnerabilities;*
- *Expand public-private partnerships to improve standards"*

And this is called "recommendations" for protecting infrastructure against HEMP in 2015, after 50 years of studying the problem?!!! It has recently become just a fashionable business to issue such recommendations.

It is not surprising that after such "recommendations" the country's infrastructure remains completely defenseless.

From the foregoing, we can conclude that military strategies, means and technologies for protecting against HEMP are too expensive for the civilian sector, and suitable strategies and technologies for the civilian sector simply do not exist now. Therefore, a new absolute different strategy and means are required for the protection of the civilian infrastructure.

Author already developed and described such a strategy and numerous technical protections means in my previous books [3.1, 3.19]. The main principles of this strategy:

- It is impossible to ensure protection of any and all types of electronic equipment in the power systems.
- It is impossible to ensure absolute protection even for the most important types of equipment being used.
- The cost of protection devices budgeted during the design stage (in case of new equipment and facilities) will be much lower compared to upgrading the existing equipment.
- Instead of protecting specific types of employed electronic equipment, it is sometimes feasible to use back-up equipment of the same type stored in a metal container directly at the facility being protected.
- Existing HEMP-simulating test benches provide insufficient information at immunity testing of the power system's electronic equipment and thus testing such equipment (e.g. each cabinet with electronic equipment) on such test-benches is not feasible.
- Due to technical and economic reasons, protection should only be provided to the most important (critical) types of electronic equipment installed at critical facilities of the power industry, rather than to any and all types of equipment employed at the power industry.
- Critical types may include equipment which is directly involved in electrical energy generation and transmission, as well as main types of relay protection, control and automation systems, AC and DC power supply systems.
- Consequently, measuring systems, communication (but not telecommunications used by digital relay protection devices), remote control and remote signaling systems do not belong to equipment without which temporary generation and distribution of electrical energy will be hampered in emergency situations.
- HEMP protection of equipment is multi-layered:
  - *he first (top) layer* includes protected buildings and structures.
  - *he second layer* includes protected rooms (halls) where equipment is installed.
  - *he third layer* includes protected cabinets with electronic equipment.

- *The fourth layer* includes protection input and output terminals of the equipment itself placed into control cabinets.
- *Some additional "layers"* of protection may include means for attenuation electromagnetic interferences penetrating into the equipment through the input and output cables (grounding, control and power).

However, the use of all these "layers" in any situation is not feasible. In some cases, it is feasible to use just some of the "layers" in various combinations.

In other words, the **general strategy** should be based on maximum use of maximum amount of known nonmilitary protection means (selected based on the above-mentioned strategy), with restrictions to be determined by technical and economic capabilities of a specific power system, only because any level of protection which can attenuate (at least partially) HEMP impact on electronic equipment is useful.

References

[3.1] Gurevich V. *Protecting Electrical Equipment: GOOD Practices for Preventing High Altitude Electromagnetic Pulse Impacts*. Berlin. DeGruyter, 2019

[3.2] Protecting America's Electric Grid Against Electromagnetic Pulse Attack. Report of Foundation for Resilient Societies, 2017.

[3.3] Baker G. Testimony of Dr. George H. Baker before the Senate Homeland Security Committee, 2019. Senate Committee on Homeland Security and Governmental Affairs, February 27, 2019.

[3.4] Cooper H. Will Biden Improve Trump's Cyber and EMP Initiatives? – *NewsMax,* 29 January 2021.

[3.5] Yates L., Gunning B. P., Crawford M.H., at al. Demonstration of >6.0-kV Breakdown Voltage in Large Area Vertical GaN p-n Diodes with Step-Etched Junction Termination Extensions. - IEEE Transactions on Electron Devices, Vol. 69, No. 4, 2022, pp. 1931 – 1937.

[3.6] TVS/Zener Theory and Design Considerations. Handbook, 2005, On Semiconductor.

[3.7] Riley K. EPRI report says existing tech would protect U.S. grid against electromagnetic pulses. – Daily Energy Insider, April 30, 2019 (https://dailyenergyinsider.com/featured/19089-epri- report-says-existing-tech-would-protect-u-s-grid-against-electromagnetic-pulses/).

[3.8] Cash C. Report: Electromagnetic Pulse Would Not Have Widespread Impact on Electric Grid. NRECA (America's Electric Cooperatives), April 30, 2019 (https://www.electric.coop/report-electromagnetic-pulse-would-not-have-widespread-impact-on-electric-grid)

[3.9] Walter J. Scientists Are Zapping Fake Electrical Grids to Help Us Survive an EMP Attack. – Discover Magazine, August 8, 2019 (https://www.discovermagazine.com/environment/scientists-are-zapping-fake-electrical-grids-to-help-us-survive-an-emp).

[3.10] Niiler E. The Grid Might Survive an Electromagnetic Pulse Just Fine. – Wired, April 30, 2019 (https://www.wired.com/story/the-grid-might-survive-an-electromagnetic-pulse-just-fine/)

[3.11] Electromagnetic Pulse Shielding Mitigations. Best Practices for Protection of Mission Critical Equipment. - Report of DHS Science and Technology Directorate, August 2022.

[3.12] Vasaka C. S. Technical Note NADC-EL-N5507: Problems in Shielding Electrical and Electronic Equipments. Naval Air Development Center, Johnsville, June 1955.
[3.13] MIL-STD-285. Attenuation measurement for enclosures, electromagnetic shielding, for electronic test purposes, method of. US Department of Defense, 15 June 1956.
[3.14] Lasitter H. A. Technical Report R-454: Construction and Evaluation of a Prototype Electromagnetically Shielded Room, Naval Civil Engineering Laboratory, Port Hueneme, June 1966.
[3.15] Lasitter H. A., Clark D. B. Technical Note N-962: Nuclear Electromagnetic Pulse Effects Design Parameters for Protective Shelters, Naval Civil Engineering Laboratory, Port Hueneme, June 1968.
[3.16] MIL-STD-907B. Engineering and design criteria for shelters. Expandable and non-expandable. US Department of Defense, 9 September 1985.
[3.17] MIL-STD-188-125. High-altitude electromagnetic pulse (HEMP) protection for ground-based C^4I facilities performing critical, time-urgent missions. US Department of Defense, 16 June 1990.
[3.18] Report AD-A275 335. EMP Design and Test Guidelines for Systems in Mobile Shelters. Army Research Laboratory, ARL-SR-1, December 1993.
[3.19] Gurevich V. Protecting Electrical Equipment: NEW Practices for Preventing High Altitude Electromagnetic Pulse Impacts. Berlin. DeGruyter, 2021.
[3.20] Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment. National Cybersecurity and Communications Integration Center, Arlington, Virginia, 2019.
[3.21] Kukjoo K. at al. Development of Decision-Making Factors to Determine EMP Protection Level: A Case Study of a Brigade-Level EMP Protection Facility. - Applied Science, 2021, No. 11, 2921. MDPI.
[3.22] Technical Report LLNL-TR-741344, Lawrence Livermore national Laboratory, 2017.
[3.23] MIL-STD-2169B. High Altitude Electromagnetic Pulse (HEMP) Environmental. Department of Defense, 2012.
[3.24] Pry V. Russia: EMP Threat. The Russian Federation's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack. EMP Task Force on National and Homeland Security, 2021.
[3.25] Cui M. Numerical Simulation of the HEMP Environmental. - IEEE Transactions on Electromagnetic Compatibility, 2013, Vol. 55, No. 3.
[3.26] Smith K., at al. Numerical Fits for Estimating High-Altitude EMP from Unclassified Gamma Ray Pulse Sources. Metatech Technical Note, 1990.
[3.27] IEC 61000-4-25. Electromagnetic compatibility (EMC) Part 4-25: Testing and measurement techniques – HEMP immunity test methods for equipment and systems, 2002.
[3.28] Electromagnetic Pulse (EMP): Thread to Critical Infrastructure. - Hearing before the Subcommittee on Cybersecurity. Infrastructure Protection and Security Technologies of the Committee on Homeland Security. One Hundred Thirteenth Congress, second session, May 8, 2014, No. 113-68.
[3.29] Apostolov A. The digital transformation. - Protection, Automation & Control World (PAC World), September 2022, p. 4.
[3.30] Apostolov A. Not IF but WHEN. From the editor. - Protection, Automation & Control World (PAC World), December 2021, p. 4.
[3.31] The Digital Substations Market Growth. Last word. - Protection, Automation & Control World (PAC World), December 2021, p. 98.
[3.32] Strategy for Protecting the Homeland Against Threats of Electromagnetic Pulse and Geomagnetic Disturbances, United States Department of Homeland Security, 2018.

[3.33] Durkovich C. Testimony of Caitlin Durkovich submitted to the Senate Energy & Natural Resources Committee. Hearing: To Examine the Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure, May 4, 2017.

[3.34] Wailes K. Statement of Kevin Wailes submitted to the Senate Energy & Natural Resources Committee. Hearing: To Examine the Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure, May 4, 2017.

[3.35] Manning R. E. Statement of Robin E. Manning submitted to the Senate Energy & Natural Resources Committee. Hearing: To Examine the Threat Posed by Electromagnetic Pulse and Policy Options to Protect Energy Infrastructure, May 4, 2017.

[3.36] Gabbard B., Joseph R. Addressing Electromagnetic Threats to U.S. Critical Infrastructure. - *JINSA's Gemunder Center EMP Task Force, JINSA, September 2015.*

Chapter IV

The Problems of Testing HEMP Resilience of Civil Equipment on Traditional Military Grade Test Benches

Introduction

Recently, it has become very important to ensure HEMP protection for civil systems that are part of a country's infrastructure, primarily, those of the power industry. In the USA for example, a special Directive signed by President D. Trump on March 26, 2019 is devoted to this issue; constantly acting Congress Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack; acting of SC77C Committee of International Electrotechnical Commission; acting WG C4.54 group within CIGRE and many other governmental, military and private companies.

Fig. 4.1. Electronic equipment controls cabinets used in the power industry

Electronic equipment used in the power industry is represented by digital protection relays (DPR), multiple controllers, systems of automation, measurement, monitoring and data transfer, as well as the SCADA system. As a rule, these are placed in a control cabinets (Fig. 4.1). The design of these cabinets is suboptimal in terms of protection from HEMP electromagnetic pulse, and thus requires significant retrofit described in [4.1, 4.2]. Such retrofit could result in rather significant complication of the cabinet's design and consequently, in cost increase. That is why it is taken for granted that the fact that efficiency of such retrofit needs to be definitely checked and confirmed experimentally.

Since E1 component of HEMP affects mostly electronic equipment, henceforth, when discussing HEMP, I mean this component exclusively.

Methods and Aims of HEMP-resilience Tests

There are two major (though not exclusive) aims of control cabinets testing:
- validation of efficiency of applied protection measures and devices;
- estimation of a minimum amount of protection devices and measures to ensure adequate level of protection.

Requirements to resilience of electronic equipment to High-Altitude Electromagnetic Pulse (HEMP) have been covered in various military and civil standards. Standards such as International Electrotechnical Commission (IEC), International Telecommunication Union (ITU) and standards of US Department of Defense (MIL-STD) are widely used internationally, Fig. 4.2.

According to basic standards applied to industrial equipment (in particular, the standards used for power industry), i.e. IEC 61000-4-25 [4.3] and ITU K.78 [4.4], the test for electronics immunity to HEMP must be divided into two parts:

- *radiated immunity test (RI)*
- *conducted immunity test (CI)*

Normally, CI is divided into two types: *pulse voltage* applied to apparatus inputs/outputs and *pulse currents* induced into equipment circuits.

Fig. 4.2. Principal international standards stipulating protection devices and methods for HEMP-resilience testing.

Testing of CI resilience is performed by means of a special HEMP simulator.

Since electronic equipment placed in the cabinets is connected with other devices by means of multiple control and power cables, and these other devices may often be located dozens and even hundreds of meters away from the cabinets, it is absolutely obvious that RI tests should be run over the whole system rather than over a separate cabinet (Fig. 4.3).

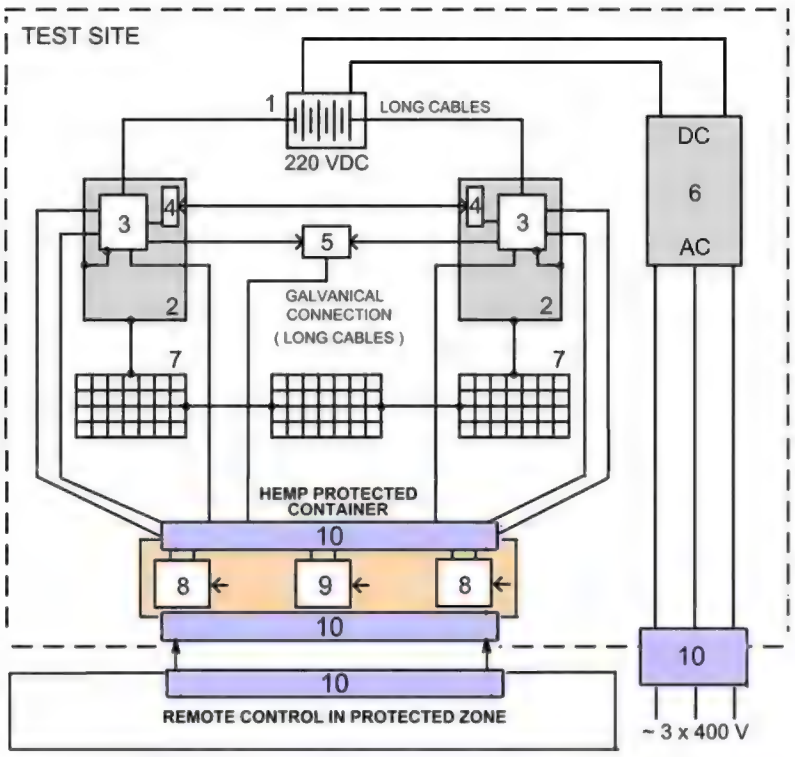


Fig. 4.3. Layout of the test-bench. 1 – Mobile battery 220V; 2 – Electrical cabinets distanced from one another; 3 – Tested electronics (such as Digital Protective Relays - DPR); 4 – Communication devices; 5 – Lockout relay controlled via DPR output circuits; 6 – Battery charger; 7 – Set of metal meshes comprising the ground system model; 8 - simulators of different modes of EUT operation synchronized or not with HEMP initiation system; 9 – EUT status recorders; 10 – HEMP Filters

The main idea of the test process was to gradually disconnect different protection elements under continuing electromagnetic pulse impacts in order to determine the minimal (optimal) number of protection elements, which would still maintain the efficiency of electronic equipment functioning (Fig. 4.4).

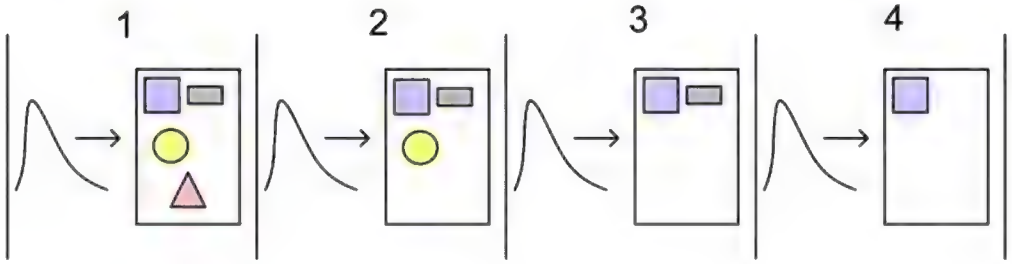


Fig. 4.4. Stages of electronic equipment testing with gradual disconnection of different protection elements and repeated generation of the test pulses.

Test Bench – HEMP Simulator

The most widely used type of RI HEMP simulators are so called guided wave-type simulators (Fig. 11.5). This simulator consists of two major parts: a source of high-voltage (several million volts) pulses and antenna system, which creates an electric field pulse (matching E1 component of HEMP) within the operational volume of the simulator, where a test object is located (Fig. 4.5). A pulse voltage generator (PVG), assembled according to Marx design, is used as a source of high-voltage pulses. A so-called bottom "plate" of this simulator represents a metal grid placed in a concrete foundation, while the top "plate" represents rows of stretched wire, supported by insulated supports.

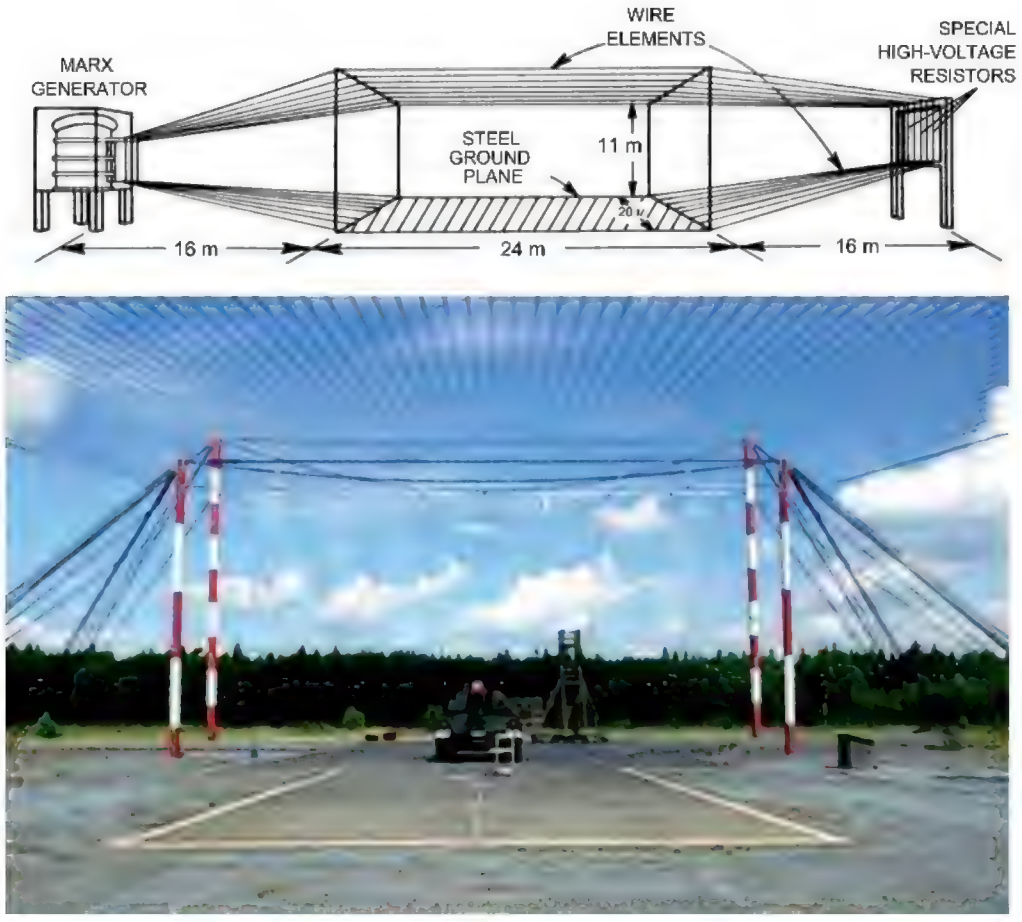


Fig. 4.5. Design and appearance of antenna system of the most widely used guided wave-type HEMP simulator.

The Problem No. 1

Since we are talking about a very short pulse (2.5/25 ns), which affects electric circuits similar to a high-frequency signal with a frequency of up to 100 MHz, obviously variations of internal layout and external cables, as well as different types of equipment used in cabinets and different combinations of this equipment, will heavily influence high-frequency properties. For example, increase of the length of connecting wires between the protection element and the electronic equipment's input terminal under protection from 25 cm to 50 cm results in full loss of

protecting capability by protection elements (e.g. varistors) [4.5]. Is it really possible to maintain strongly identical wiring and short connecting wires in all the cabinets with different electronic equipment inside? The answer is pretty straightforward: not at all. Therefore, does not make any sense to extrapolate the findings obtained for one cabinet to other cabinets.

What should we do with testing of military systems on such benches? The fundamental difference of military systems (armored fighting vehicles, aircrafts, missiles), which are obligatory subjected to such tests, is that each one of these systems are enclosed and autonomous and all of their cables run inside, without stretching for hundreds of meters outside. Secondly, all copies of the same type are manufactured based on the same drawings with strict adherence to the same technology. They feature negligibly small differences both in terms of component parts and in terms of assembly, which is performed using the same wire harness that has been previously prepared on a special's templates. Thirdly, the circuits of internal electronic equipment are irrelevant to the earth and its potential. These features of military equipment make it possible to test it on existing test benches and extrapolate the findings obtained for one sample over the total batch of this type.

Cabinets with electronic equipment used in the power industry may differ in terms of design, may contain long cables stretching outside for hundreds of meters and running inside, and may be equipped with obligatory earthing.

Since we are talking about a very short pulse (2.5/25 ns), which affects electric circuits similar to a high-frequency signal with a frequency of up to 100 MHz, obviously variations of internal layout and external cables, as well as different types of equipment used in cabinets and different combinations of this equipment, will heavily influence high-frequency properties, and consequently equipment sensitivity to HEMP and efficiency of protection elements [4.2], that it does not make any sense to extrapolate the findings obtained for one cabinet to other cabinets. Moreover, existing test benches do not provide a real picture for equipment using external earthing.

This challenges feasibility of electronic equipment testing on test benches which simulate HEMP. In my opinion, as of today we have already accumulated certain experience in the field of development of protection means for electronic equipment -; there are descriptions of component parts and materials which are different from those used in military equipment in terms of their cost. Of course, efficiency of these protection measures will be much lower than that of armored fighting vehicles or missiles, but in its combination, its will be enough for preventing damage to the majority of types of power industry electronic equipment.

The fundamental difference of military systems (armored fighting vehicles, aircrafts, missiles), which are obligatory subjected to such tests, is that all copies of the same type of equipment are manufactured based on the same drawings with strict adherence to the same technology. They feature negligibly small differences both in terms of component parts and in terms of assembly, which is performed using the same wire harness that has been previously prepared on a special template.

The Problem No. 2

The problem is that it is impossible to simulate HEMP impact on hundred-meter long control cables using a test-bench with 15 by 20 meters bottom plate (or similar to that). How would you accommodate long cables in such a restricted area? If a zigzag pattern is used, the pulse induced in oppositely directed parts of the zigzag will be mutually compensated. If they are placed in

concentric circles, the impact of the test-bench's electric field onto this cable will be significantly higher compared to the real situation. Combination of the two is both too complicated for calculations and almost unpredictable.

If the object being tested features short cables, sometimes the way out would be to increase the intensity of the simulator's electric field (determined theoretically) in order to obtain the outcome similar to long cables. It should be noted though that intense electric field will impact both short cables and all other items placed in the working space, e.g. control cabinets, and this is unacceptable. Placement of short cables outside the working area of the simulator (in the area of stronger fields) is also not a solution to the problem, since outside the working area the electric field is not equivalent at different points.

The Problem No. 3

There is a problem of how to adjust the strength of the simulator's electric field during testing. The findings of computer simulation reported by Lawrence Livermore National Laboratory LLNL-TR-741344 [4.6] suggest that the voltage amplitude on the ends of 45 and 65-meter-long control cables can reach as high as 100 – 120 kV at established rating of RI HEMP's electric field of 50 kV/m. This means that a high voltage such as this can be applied to inputs of electronic equipment to which these cables are connected. On the other hand, does this mean that electronic equipment should really be subject to tests designed for such a significant voltage? Alternatively, let us say: do we really need to use field strength of 50 kV/m (stipulated by standards) during simulation tests, even though it causes very high voltage on control cables used for testing (and inputs of electronic equipment)? Let us consult with standards to find the answer.

The main standard IEC 61000-4-25 establishes the amplitude of the pulse voltages at the inputs of the equipment, as well as the electric field strength during the tests, depending on the actual placement and degree of protection of the equipment (test concept) to be tested.

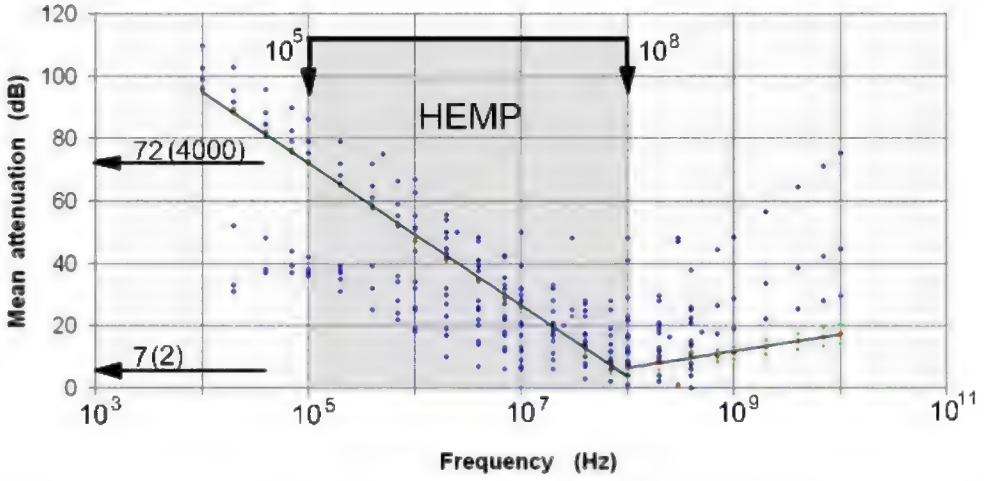


Fig. 4.6. The trend of shielding ability of reinforced concrete buildings depending on the electromagnetic emission frequency (IEC 61000-4-36)

Determination of proper test concept (out of 6 available) is the first step for defining the rules for a certain test. Standards 61000-2-11 [4.7] and 61000-5-3 [4.8] describe these concepts. Concept 2b can be suitable for the EUT located inside the major reinforced concrete or all-brick

building protected against lightning, but having no special protective filters. This concept allows for attenuation of EUI by 20 dB in the frequency band of 100MHz–30MHz due to the building structure. For this concept and for component E1, the strength of the radiation electrical field acting upon the tested equipment should be equal to 5kV/m (level R4). Let us compare: for wooden buildings, providing zero EI attenuation, the strength of the electrical field equals to 50 kV/m (level R7).

The next step is to choose the CI test level according to IEC 61000-4-25. For the concept 2b, due to the presence of cables connected to the tested facility and not buried in the ground, the level of test impact should correspond to E8 (to allow for 50% probability of the facility immunity) or E9 (to allow for 99% probability). For E8 level, it is assumed that the tested facility is immune to the pulse voltage of 8kV, and for E9 level – to the pulse voltage of 16kV. A probability of 50% is deemed as normal according to the standard and can be applied to the civil equipment.

Thus, the standards suggest that the field strength adjusted on the simulator should be 5 kV/m. But there are only few simulators which offer technical possibility to adjust such low rates of field strength. Secondly, thorough studying of HEMP weakening phenomenon by real buildings and structures makes me question the standards, which suggest HEMP weakening at 20 dB (i.e. 10-fold).

In the IEC 61000-4-36 [4.9] standard is shown (as the trend) the shielding ability of reinforced concrete buildings depending on the electromagnetic emission frequency, including for the frequency range corresponding to the HEMP, Fig. 4.6. The data obtained from numerous measurements. From Fig. 4.6 it can be seen that in the frequency range characterized the HEMP (10^5 - 10^8 Hz), the attenuation level by the building can change 2000 times from the beginning to the end of the frequency range! With such changes, accurate measurements of attenuation by a specific building will give little. In addition, basic instruments for measuring such attenuation [4.2] are designed to measure the properties of panels of a small area, such as a wall, a door, a window, and not the entire building.

Placement of electronic equipment within the room (e.g. in relation to a window or a door) can also significantly impact the rate of emission weakening. Furthermore, positioning of the district, where the building with equipment is situated relative to the Earth poles and the Equator, can also significantly influence the actual strength of HEMP's electric field affecting the equipment [4.2].

So, which value of electric field strength should we set up on the simulator during testing?

The Problem No. 4

Earthing of cabinets and electronic equipment inside them is another issue to be addressed. This issue is determined on the one hand by the difference between electromagnetic pulse of lightning (LEMP) and that of a high-altitude nuclear explosion (HEMP), and on the other hand, by the design of the test-bench with an earthed bottom plate.

LEMP is a local pinpoint electric discharge between two electrodes: a cloud and an object with earth potential (or earthing system). Whereas HEMP is not a pinpoint, but a rather extensive physical process determined by electrons quickly flowing towards earth and covering an area of thousands of kilometers.

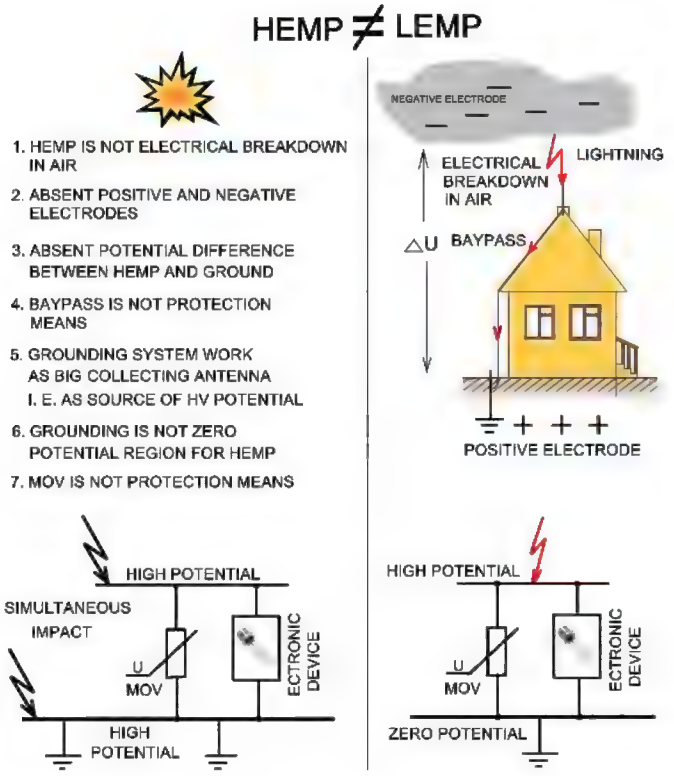


Fig. 4.7. The difference between HEMP and electromagnetic pulse of lightning (LEMP).

The nature of these events is absolutely different, Fig. 4.7 and thus the response of electrical conductors to their impact will also be different [4.2, 4.10]. For example, imagine a long metal rod placed on two insulators with negligibly small capacitance to earth (Fig. 4.8). In case LEMP impacts one of its ends and the other end will be earthed, a current pulse determined by high potential difference between the rod's ends will run through the rod.

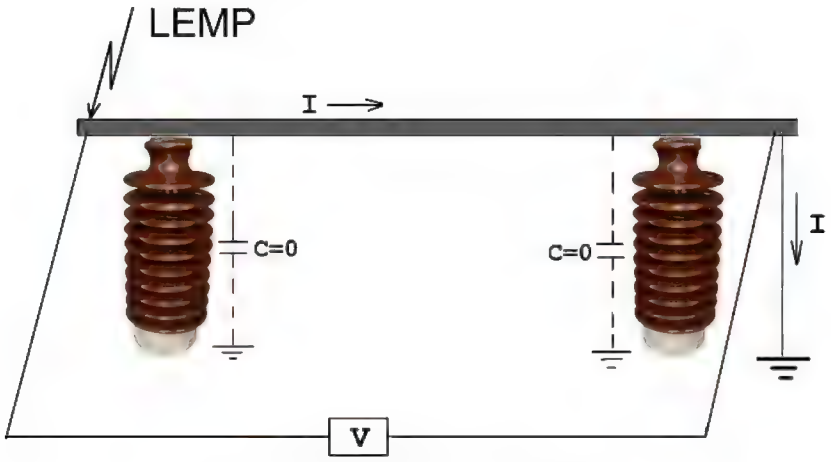


Fig. 4.8. LEMP impact onto metal rod

Will there be a potential difference between the rod's ends and will a current pulse run through it, if the right end of the rod will be disconnected from the earth? The answer is obvious: No. Thus, earthing is very important upon LEMP impact.

Now, let us address the effect of earth upon HEMP impact (Fig. 4.9).

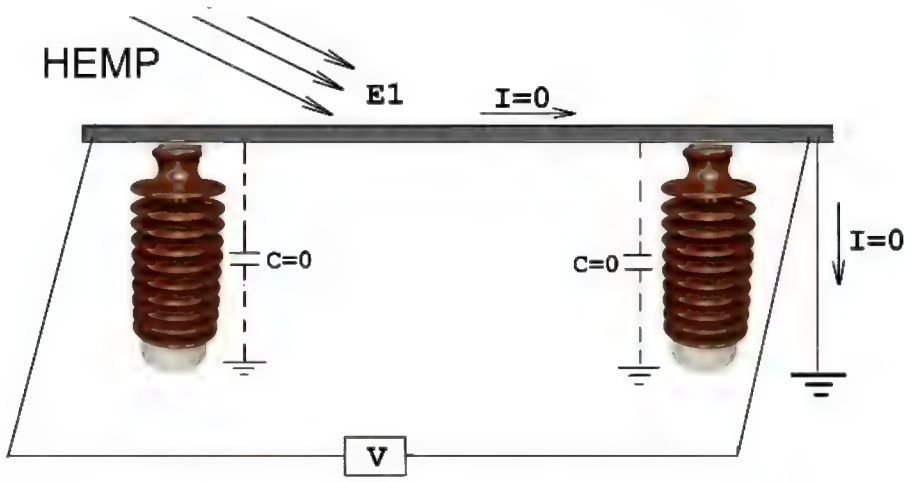


Fig. 4.9. Impact of HEMP (its E1 component, to be precise) onto a metal rod

Upon HEMP impact, high potential difference occurs between the rod's ends regardless of whether or not the earthing is available. There will be no current, even if the earthing is there, since this potential difference is irrelevant to the earth potential. This is very similar to a battery insulated from the earth (e.g. hanging on an insulation strand) (Fig. 4.10). The potential difference between the battery's terminals will not depend on the earth availability. In addition to that, earthing of one of the terminals will not lead to current occurrence in the earth circuit. This means that upon HEMP impact an insulated rod will be as indifferent to earthing as an insulated battery.

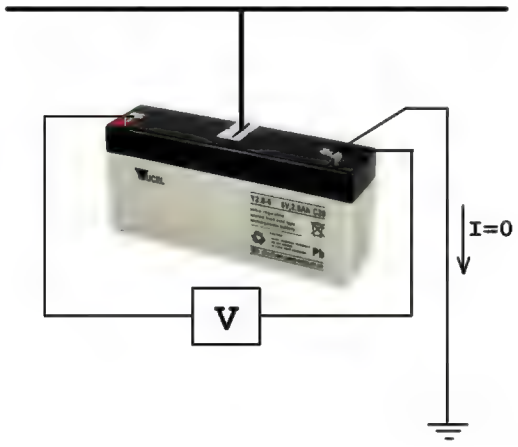


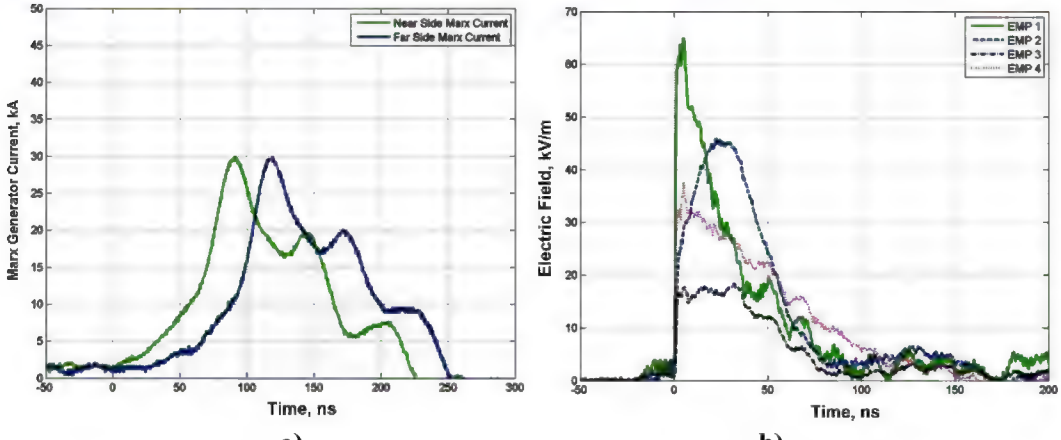
Fig. 4.10. Current rates and voltages in the battery insulated (hanging on insulation strand) from the earth

Now, let us return to the HEMP testing bench (Fig. 4.5). Since the pulse of high-density electric field occurs in the guided wave-type simulator between the top insulated electrode and the bottom earthed electrode, obviously the earthed test object placed between these electrodes will respond like being struck by LEMP rather than by HEMP. In other words, such a simulator with

earthed equipment placed inside simulates lightning strike, but not the impact of a high-altitude nuclear explosion. It should be noted though that earthing of the test object's metal body, e.g. the cabinet (i.e. balancing of its potential with that of the bottom plate) creates a bypass for induced current similarly to a lightning rod connected to earthing upon a lightning strike. Additionally, connection of surge protection devices between circuits of electronic equipment and the earth (i.e. the bottom plate of the simulator) will significantly weaken the impact of the test pulse (like earthing upon a lightning strike) and this can be wrongly perceived as an efficient protection against HEMP. Under real conditions, the potentials induced by HEMP in conducting elements are not connected with the earth's potential and thus earthing availability does not affect HEMP resistance of equipment. This means that use of guided wave-type simulators for electronic equipment (earthed under real conditions) testing is not practical as this distorts the real picture of HEMP impact.

The solution would be to switch to other types of simulators, so called "hybrid" simulators. This simulator also includes the Marx design pulse generator with an output voltage of several million volts, but this generator is much smaller and is powered by a chargeable accumulator battery. The generator is fixed at a certain height in the middle part of an antenna system, made up of a large biconical antenna with two long round cross-section flat cables, made up of wire mesh. These simulators can be both stationary and mobile (Fig. 4.11).

Fig. 4.11. Hybrid-type simulators: stationary (left), mobile (right).



a) b)

Fig. 4.12. Parameters of PS-6 hybrid type simulator: a – generator's currents registered close to (left) and far away from (right) the generator; b – electric field created by antenna system at different settings of the generator [4.13].

Unfortunately, there are very few simulators of this type and they are used less frequently compared to guided wave-type simulators. In fact, guided wave-type simulators are marketed as equipment primarily used for testing aircrafts and missiles in flight, whereas hybrid-type simulators are designed for testing ground-based equipment (i.e. electronic equipment addressed in this chapter).

The important advantage of such simulators is that their antenna system can be insulated from the earth [4.11]. However, even if it is earthed for better antenna balancing, the potential induced in the test object is not connected with that of the earth. Yet, according to [4.12], hybrid-type simulators create much weaker electric field (several kilovolts per meter) intended for testing shielding shells efficiency, and thus they cannot cause actuation of non-linear surge protection elements, such as varistors. According to [4.12], such simulators cannot be used for checking efficiency of equipment protection provided by non-linear surge protection elements. Contrary to the above, [4.13] suggests a description of a PS-6 hybrid-type simulator based on two interconnected portable Marx generators with output voltage of 3 million Volts each, installed at Naval Air Station Patuxent River in 2010. This simulator resembles other hybrid-type simulators (Fig. 4.11), but unlike previous designs it provides much higher field intensity values in its working volume (Fig. 4.12).

According to [4.13] this simulator can create an electric field of up to 77 kV/m in its working area as far as 24 meters away from the generator. The problem is that this simulator exists in a single copy so far.

The Problem No. 5

Next problem is using the requirements of the MIL-STD-188-125-1 [4.14] concerning injection of current pulse at testing resilience of electronic equipment to HEMP.

These requirements have been covered in various military and civil standards. Civil standards such as International Electrotechnical Commission (IEC) and International Telecommunication Union (ITU) and military standards of US Department of Defense (MIL-STD), Fig. 4.2, are widely used internationally.

As mentioned above, according to basic standards applied to industrial equipment, (particularly the standards used for power industry) i.e. IEC 61000-4-25 [4.3] and ITU K.78 [4.4], the test for electronics immunity to HEMP must be divided into two parts:

- *radiated immunity test (RI)*
- *conducted immunity test (CI)*

Normally, CI is divided into two types: *pulse voltage* applied to apparatus inputs/outputs and *pulse currents* induced into equipment circuits.

Common standard IEC 61000-4-25 [4.3] is based on IEC 61000-4-4 [4.15], which deals with electromagnetic compatibility and does not even mention testing with a pulse current. On the other hand, IEC 61000-4-25 [4.3] describes the current as "short circuit currents for common mode" (160A and 320A, respectively for immunity test level EC8 and EC9 [4.3]). According to p. 8.4 of the standard IEC 61000-4-25, "the tests are required for all types of conductive lines… and shielding cables". The standard does not contain a definition for the term "*conductive lines*", and it seems that it does not discuss current injection into input circuits of electronic equipment.

ITU K.78 [4.4] standard also deals with control and communication cable shield tests.

Nonetheless, when testing HEMP-resilience of equipment, a reference is often made to MIL-STD-188-125-1 [4.14], which stipulates the necessity to test by current injection into internal circuits of electronic equipment. Is it really necessary?

Unlike the above-mentioned standards, MIL-STD-188-125-1 suggests a little different interpretation of the CI test. It includes a separate section called "Pulsed Current Injection (PCI) Test Procedures" (Appendix B). The problems with this section are obvious from the very beginning, i.e. regarding the Definitions sections. The tests in this standard are divided into two sub-types: acceptance testing и verification testing:

> *«B.1.2 Applications. These procedures shall be used for **acceptance testing** after construction of the HEMP protection subsystem and for **verification testing** of electrical POE protective treatments after the facility is completed and operational (POE – point of penetration)».*
>
> *«Acceptance testing... to demonstrate that electrical POE protective devices, as-installed, perform in accordance with the transient suppression/ attenuation requirements of this standard»*
>
> *«Verification testing... to demonstrate that mission-critical systems (MCS) are not damaged or upset by residual internal transient stresses».*

It seems to be logical, but there are no further explanations to this logic, see Table 4.1.

Table 4.1. Definition of the Pulsed Current Injection (PCI) Test Procedures in the standard MIL-STD-188-125-1 [4.14]

Purpose of the acceptance test (B.4.2.1)	**Purpose of the verification test (B.4.2.2)**
a. To measure the performance of as-installed conductive POE protective devices.	a. To measure the performance of conductive POE protective devices in operational circuit configurations.
b. To demonstrate through post-test inspection, performance checks, and response data analysis that the protective devices not be damaged or degraded by threat relatable transients.	b. To demonstrate through post-test inspection, performance checks, and response data analysis that the protective devices will not be damaged or degraded by threat-relatable transients.
c. To identify defective devices or faulty installation practices, so that repairs or replacements can be made.	c. To identify defective devices or faulty installation practices, so that repairs or replacements can be made.
-	d. To characterize the residual internal transient stresses
-	e. To demonstrate that residual internal transient stresses will not cause mission aborting damage

	or upsets of the MCS in their various operating states.
-	f. To provide data for HEMP hardness assessment of the facility and baseline data for the hardness maintenance/hardness surveillance program.

Clauses "a" through "c" are completely identical, while clauses "d" through "f" explain and clarification clause "c". Considering these explanations, it becomes unclear why requirements of this standard have been divided into "Acceptance test" and "Verification test". Moreover, all tests are to be conducted relative to the ground ("common mode") and no tests have been elaborated for a so called "differential mode". In other words, between terminals of the same input or output, as well as between different inputs and outputs as stipulated in all EMC standards. Why? There is no explanation of this phenomenon in the standard.

It is noteworthy that the above-mentioned definitions refer to "***conductive** POE protective devices*", whereas the values of pulse currents are given (see B.4.5) for shortened circuits as "***short-circuit currents***":

> *"... pulse generator requirements are defined in terms of short-circuit current and source impedance.* ***Short-circuit current is defined as current driven through a short circuit connected to the generator output"****.*

Nevertheless, power supply circuits, as well as input and output circuits of electronic equipment, are not "conductive short-circuits" by any means and feature rather high impedance. So how should we test them?

Table B-I of this standard stipulates technical requirements for testing equipment, particularly for a high-voltage pulse generator. This device should generate a current pulse with an amplitude of up to 5,000 A with the source impedance of 60 Ω. According to the standard: "source impedance is the ratio of the generator peak open-circuit voltage to the peak short circuit current", i.e.: $R_{SOURCE} = U_{OPEN}/I_{Sh.C.}$. Thus, the requirement to "open-circuit voltage" can be determined as: $U_{OPEN} = R_{SOURCE} \times I_{Sh.C.} = 60\Omega \times 5{,}000\ A = 300{,}000\ V$. The generator provides such parameters are really existing on the market. For example, Marx type generator, manufactured by Montena EMC company [4.16].

In other words, output voltage of the generator, the output terminal which is connected to a circuit with high source impedance, (such as inputs/outputs of low-voltage electronic equipment) can reach as high as hundreds of thousands of volts! Which electronic circuits could sustain this voltage? Why should this voltage be applied to these circuits as they are subject to civil standards [4.3, 4.4] restricting voltage at 8 kV (level EC8) or 16 kV (level EC9), depending on specific placement of equipment?

These simple calculations, multiple references to conductive circuits and short-circuit currents, as well as lack of tests for "differential mode", imply that the requirements of this section are not applicable for electronic equipment. They are rather suitable for testing of conductive protection devices, such as filters, which are connected into a "common mode", and grounded cable shields. I assumed this previously and thus I did not mention pulse current tests as a recommended (see [4.1, 4.2]) method of HEMP-resilience testing of electronic equipment.

However, some specialist dealing with these tests insists on adhering to requirements of this section of MIL-STD-188-125-1 when testing electronic equipment. It is globally true that HEMP simulators are usually maintained by military men or military industry representatives. They used to work with military standards and may often have no idea about existing sets of civil standards. When civil specialists test civil equipment on military test benches, they have no choice but to accept the rules established by the owners of the testing equipment. Hence, a supposed necessity of testing civil equipment based on MIL-STD-188-125-1 is also suggested in various scientific and technical papers. This is the reason why this research was necessary to challenge a common opinion.

Let us now address the necessity of using this section of MIL-STD-188-125-1 for electronic equipment protected by transient voltage suppressors, such as varistors connected parallel to input/output terminals. Parameters of varistors are known as they are published in their data sheets (e.g., see Table 4.2).

Table 4.2 Main parameters of some 14 mm diam. varistor types

Type/Manufacturer	**Littelfuse**	**Epcos**	**Vishay**	**Bourns**
Varistor's Type	V320LA 20CP	S14K320E2	VDRS14T320xyE	MOV-14D511K
Diameter, mm	14	14	14	14
Max. Operating AC Voltage, V_{RMS}	320	320	320	320
Varistor Voltage, V	558	510	510	561
Max. Absorption Energy, J	165	136	120	125
Max. Pulse Current (8/20 µs), A	6500	6000	4500	4500
Clamping Voltage, V	850	840	842	845

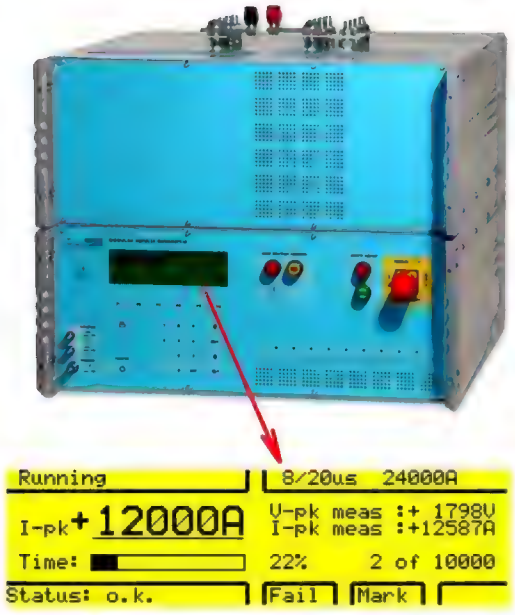


Fig. 4.13. Parameters of test pulse registered by internal measuring circuit of MIG0624 generator (screenshot).

When necessary, they can be tested separately by means of different pulse generators without any connection to the electronic equipment which they are designed to protect. The only thing that needs to be done is just to have a current pulse of a required amplitude run though this protection element and to measure the residual voltage on it.

Below is an example of measuring residual voltage on a 20 mm diam. varistor S20K275E3K1 type. Though its maximum rated pulse current is 12,000 A, it was subjected to a current pulse with an amplitude of about 12,500 A, obtained by means of a standard pulse (8/20 μs) generator MIG0624 (EMC-Partner), Fig. 4.13.

Obviously, this high pulse current amplitude results in significant residual voltage (almost 18 kV). Nevertheless, it should be considered that this current rating is much higher than the requirement of MIL-STD-188-125-1 (Table B-II).

Regarding the E1 component of HEMP, the standard stipulates 5,000 A for conducting protective shields, including cable shields. For other types of equipment, (which exactly?) the standard establishes an amplitude of up to 2,500 A. Clearly, when the amplitude of current pulse is much lower than 12,000 A, residual voltage will also be lower and additional ferrite filters mounted on the penetrated cables [2] reduce it even further.

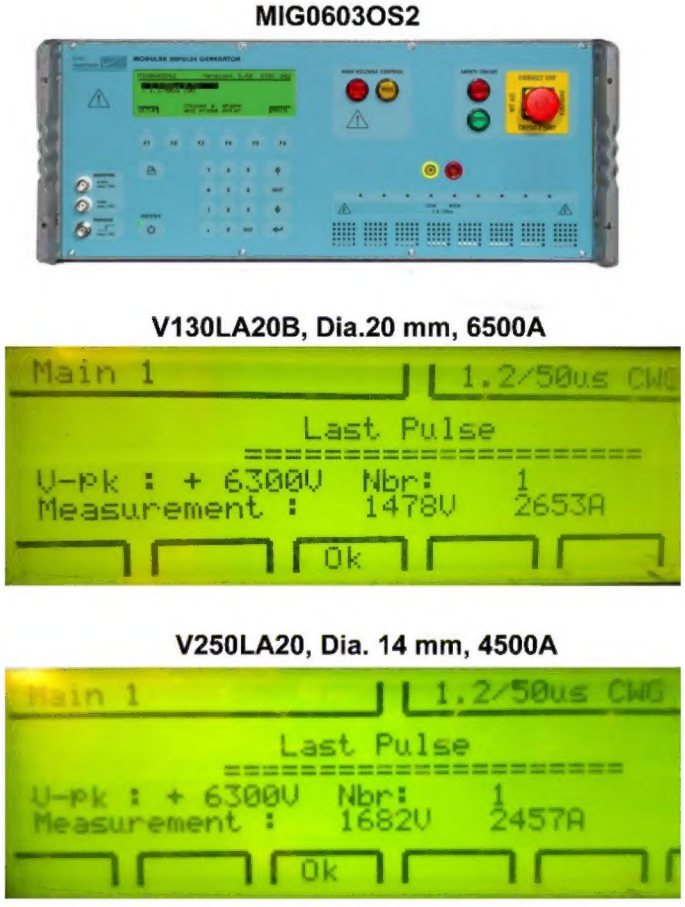


Fig. 4.14. Screenshots of MIG0603OS2 pulse generator when testing varistors V250LA20 (14 mm) and V130LA20B (20 mm) with maximum rated pulse current at 4,500 A and 6,500 A, respectively.

For example, Fig. 4.14 shows screenshots of a MIG0603OS2 pulse generator testing 14 mm and 20 mm diam. varistors by supplying a pulse current with 2,500 A amplitude. The varistors are connected to the generator's output by means of an ordinary 0.5-meter-long wire harness which simulates real placement layout in a cabinet; at the same time the residual (clamping) voltage on the varistors does not exceed 1,700 V.

A filter with ferrite rings placed over a control cable before the varistor (Fig. 4.15) introduces additional pulse weakening due to circuit impedance increase. Use of this filter is recommended in [4.2] as an imperative technical means for protecting electronic equipment in control cabinets.

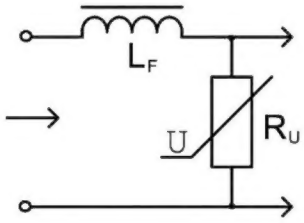


Fig. 4.15. Equivalent circuit for ferrite filter (L_F) and varistor (R_U) connection.

Connecting a 1-meter-long wire to a generator's output results in a current pulse flowing in a wire featuring 450 A at 150 V (see screenshots in Fig. 4.16). However, if six ferrite rings are placed on this wire, the same current rating will be achieved at 590 V, meaning almost 4-fold increase of impedance.

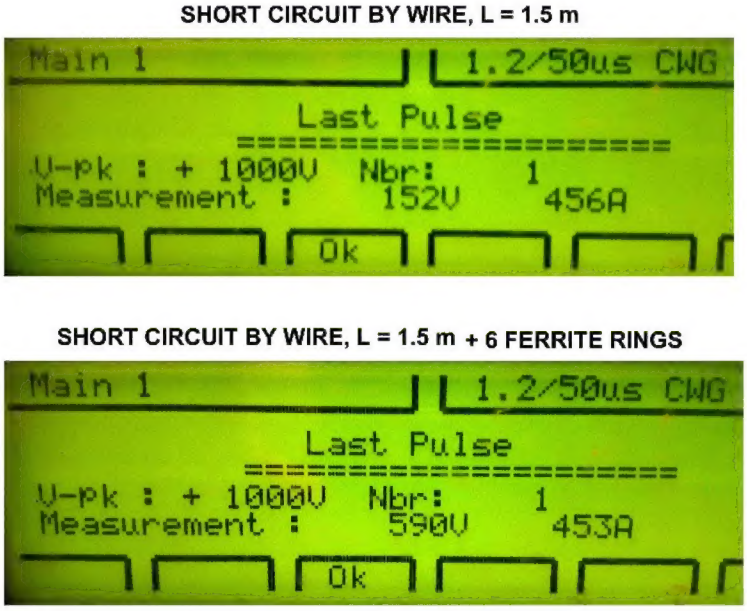


Fig. 4.16. Screenshots of MIG0603OS2 generator when short-circuiting its output by 1-meter-long wire (top) and when placing additional six ferrite rings over this wire (bottom).

One-two kilovolt voltage applied to electronic equipment inputs (when rated pulse current flows through additional external transient voltage suppressing element placed at the input) are acceptable for industrial electronic equipment, as this meets the requirements of common standards on electromagnetic compatibility.

This means that industrial electronic equipment will be automatically resilient to current pulse flowing through input protecting elements upon HEMP impact, if it is protected from HEMP voltage pulse by adding an external transient voltage suppressing elements, such as varistors, and meets the requirements of civil standards on electromagnetic compatibility. Thus, there is no need to carry out additional tests on special testing equipment stipulated by MIL-STD-188-125-1.

Conclusions

1. The need to protect a country's infrastructure (power industry assets in the first place) from electromagnetic pulse of high-altitude nuclear explosion (HEMP) impact makes it necessary to test HEMP-resilience of contemporary electronic equipment of automation, control and relay protection. However, this equipment, which constitutes a complex branched system and is placed in special cabinets, differs from military equipment in some aspects. These differences make it difficult or even impossible to use existing test methods and HEMP simulators designed for military equipment testing. Lack of test methods and testing equipment suitable for branched power industry's systems of automation, control and relay protection suggests that these tests are currently impractical in view of the available testing equipment.

2. Requirements of section B "Pulsed Current Injection (PCI) Test Procedures" of MIL-STD-188-125-1 are not suitable for testing civil electronic equipment by supplying test pulses to its input and output terminals. Thus, these tests should be excluded from the testing schedule of this equipment to HEMP-resilience. Industrial electronic equipment, meeting the requirements of standards on electromagnetic compatibility, will also be resilient to current pulse flowing through additional input-placed transient suppression protecting elements upon HEMP impact, and thus requires no additional tests to be carried out on special testing equipment stipulated by MIL-STD-188-125-1.

3. HEMP Protection Strategy for power system's electronic equipment, described in Chapter 5, must be used instead of testing civil control cabinets on military HEMP test branches.

References

[4.1] Gurevich V. Protection of Substation Critical Equipment Against Intentional Electromagnetic Threats. – Wiley, Chichester (UK), 2016, 228 p.

[4.2] Gurevich V. Protecting Electrical Equipment: Good Practices for Preventing High Altitude Electromagnetic Pulse Impacts. – De Gruyter, Berlin, 2019, 386 p.

[4.3] IEC 61000-4-25 Electromagnetic compatibility (EMC). – Part 4 – 25: Testing and measurement techniques. – HEMP immunity test methods for equipment and systems.

[4.4] ITU-T K.78 Series K: Protection against interference. High altitude electromagnetic pulse immunity guide for telecommunication centers. Recommendation ITU-T, 2016.

[4.5] Gurevich V. HEMP Protection of Electronic Equipment Located in Control Cabinets. – International Journal of Research Studies in Electrical and Electronic Engineering (IJRSEEE), 2019, Vol. 5, Iss. 1.

[4.6] Technical Report LLNL-TR-741344. Project FOOTPRINT: Substation Modeling and Simulations for E1 Pulses / S. D. Nelson, D. J. Larson, B. A. Kirkendall. – Lawrence Livermore National Laboratory, 2017.

[4.7] IEC 61000-2-11 Electromagnetic compatibility (EMC)—Part 2–11: Environment—Classification of HEMP environments.

[4.8] IEC/TR 61000-5-3 Electromagnetic compatibility (EMC)—Part 5–3: Installation and mitigation guidelines—HEMP protection concepts.

[4.9] IEC 61000-4-36 Electromagnetic compatibility (EMC) - Testing and measurement techniques - IEMI Immunity Test Methods for Equipment and Systems.

[4.10] Gurevich V. Testing HEMP Resilience of Electronic Equipment Used in Power Industry: Is It Essential? – International Journal of Research and Innovation in Applied Science, 2019, Vol. IV, Iss. V.

[4.11] Baum C. E. EMP Simulators for Various Types of Nuclear EMP Environments: An Interim Categorization. – IEEE Transactions on Electromagnetic Compatibility, 1978, Vol. EMC-20, No. 1.

[4.12] Prather W. D., Giri D. V. Spectrally Flat Antenna Design and Reshaped TEM Horns. – Sensor and Simulation Notes, Note 579, 2018.

[4.13] Belt D., Mazuc A., Sebacher K., Bailey V., and etc. Operational Performance of the Horizontal Fast Rise EMP Pulser at the Patuxent River EMP Test Facility. – IEEE Pulsed Power Conference, Chicago, USA, 19-23 June 2011.

[4.14] MIL-STD-188-125-1 High –Altitude Electromagnetic Pulse (HEMP) Protection for Ground Based C^4I Facilities Performing Critical. Time-Urgent Mission. Part 1 Fixed Facilities, 2005.

[4.15] IEC 61000-4-4 Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test, 2004.

[4.16] Pulsed Current Injection Test System According to MIL-STD-188-125/1 & 2. System Description. Montena EMC, 2008.